Generalized Channel Probing and Generalized Pre-Processing for Secret Key Generation

Yingbo Hua, *Fellow, IEEE*

***Abstract*—The paper considers secret key generation (SKG) from a channel between Alice and Bob against Eve all with multiple antennas. A generalized channel probing (GCP) method and a generalized pre-processing (GPP) method are proposed as two major steps before quantization, information reconciliation and privacy amplification for SKG. The degree-of-freedom (DoF) of the secret key capacity (SKC), relative to power or signal-to-noise ratio, based on the data sets at Alice, Bob and Eve after the execution of GCP is shown. The SKC-DoF is also shown to be the same as that based the new data sets after the application of GPP except for modifications chosen for computational efficiency. In particular, if Eve has a less number of antennas than either Alice and/or Bob, the SKC-DoF grows with the number of random transmissions from either Alice and/or Bob within each channel coherence period. This SKC-DoF property for GCP and GPP does not require the reciprocity of the channel. A reciprocal channel simply adds a product of the numbers of antennas at Alice and Bob towards the total SKC-DoF. Also shown in this paper is GCP with embedded public pilots, which results in no loss of SKC-DoF. Two prior methods for channel probing are also reviewed, and it is shown that none of them has the above mentioned SKC-DoF property despite previous claims. The potential application areas of GCP and GPP include both wireless and wireline networks.**

***Index Terms*—Network security, secret key generation, secret key capacity, degree of freedom, channel probing, pre-processing.**

I. Introduction

FOR current and future networks such as Internet-of-Things and Internet-of-Everything, security for authenticity, privacy, integrity, etc, can be all enhanced by the availability of fresh secret keys between legitimate parties. Due to the massive numbers of nodes in current and future networks, reliable and timely key distributions via central operators are often impractical. This makes secret key generation (SKG), especially opportunistic SKG from any available channel environment, a problem of great importance. A secret key generated from a wireless or wireline channel between two parties can be later used anytime and anywhere for security purposes between them. For a comprehensive review of SKG, see recent survey articles such as [1], [2].

Manuscript received 21 November 2022; revised 11 February 2023; accepted 9 March 2023. Date of publication 20 March 2023; date of current version 7 April 2023. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Yuxin Chen. This work was supported in part by the Department of Defense under Grants W911NF-17-1-0581 and W911NF-20-2-0267.

The author is with the Department of Electrical and Computer Engineering, University of California at Riverside, Riverside, CA 92521 USA (e-mail: yhua@ee.ucr.edu).

Digital Object Identifier 10.1109/TSP.2023.3259142

It has become a widely accepted notion since [3] that if a channel between Alice and Bob is reciprocal within a coherence period, then the channel can be first probed with (public) pilots by Alice and Bob to obtain their respective estimates of the channel response. Then, they can perform any of the well established methods for quantization, information reconciliation and privacy amplification to produce a secret key [1], [2]. The achievable secret key rate in bits per second using the above approach is known to be limited in proportion by the inverse of the channel coherence time. For environment with long coherence time, the above approach may not meet practical needs.

Recently, there have been attempts to increase the secret key rate beyond that constrained by the channel coherence time. The authors of [4] proposed that for each coherence period, a single-antenna Alice sends a sequence of random symbols to a single-antenna Bob, and Bob sends another sequence of random symbols to Alice. The authors claimed that a higher secret key rate unconstrained by the channel coherence time can be achieved this way. The authors of [5] considered a multi-antenna Alice and a single-antenna Bob and proposed that Alice sends sequences of random symbols via her randomly selected antennas sequentially to Bob, and Bob sends a (public) pilot to the randomly selected antennas at Alice. The authors claimed that their approach can also achieve a secret key rate unconstrained by the channel coherence time.

In this paper, we will show that in terms of the degree of freedom (DoF) of the secret key capacity (SKC), none of the two approaches in [4] and [5] outperforms the standard methods where both Alice and Bob only send to each other public pilots. See Sections II-A1 and XI.

It is important to note that SKC can be generally expressed as $d \log P + c$ at a high transmission power P where the constant $d \geq 0$ is the DoF of SKC (relative to P), which is the primary (or first-order) measure of how good a SKC is. The constant c is the secondary (or second-order) measure of SKC, which is useful to compare two or more SKCs when they have the same DoF. The physical meaning of DoF can be also appreciated from the differential entropy $h(\mathbf{v}|\mathcal{Z})$ of a "secret" $n \times 1$ complex Gaussian vector $\mathbf{v}$ with power P for each entry, conditional on enemy's observation $\mathcal{Z}$. It can be shown that $DoF(h(\mathbf{v}|\mathcal{Z}))$ equals n if $\mathbf{v}$ given $\mathcal{Z}$ consists of independent entries or has a full-rank covariance matrix, or equals one if $\mathbf{v}$ given $\mathcal{Z}$ consists of fully correlated entries or equivalently has a rank-1 covariance matrix.

More broadly, this paper presents a generalized approach for channel probing and pre-processing before the quantization step takes place for SKG. Unlike the major steps often stressed in the literature such as in [1], [2], here we stress the importance of both channel probing and pre-processing as shown in Fig. 1. We define "channel probing" as the first step that results in the

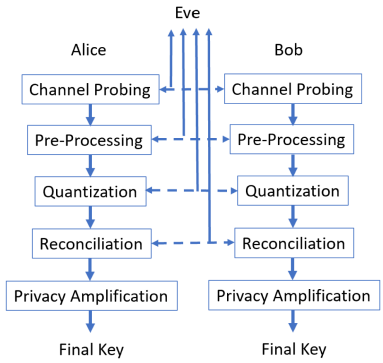

Fig. 1. Major steps in SKG. The dashed arrows represent public or semi-public communications between Alice and Bob that leak certain amount of information to Eve.

initial sets of data, i.e., $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$, available to Alice, Bob and Eve (eavesdropper) respectively. In general, there may be no direct correspondence between the elements in $\mathcal{X}$ and those in $\mathcal{Y}$, and hence the established methods for quantization may not be readily applicable. We define "pre-processing" as the step that uses $\mathcal{X}$ and $\mathcal{Y}$ to yield a pair of highly correlated secret vectors at Alice and Bob that are ready to be quantized into a pair of highly correlated bit streams. Such quantization methods include coset based quantization [6], guard-band based quantization [7] and continuous encryption based quantization [8], [9]. These bit streams can be then converted by information reconciliation and privacy amplification, using methods such as in [2], [4] and [10], into a final secret key. Furthermore, we allow "pre-processing" to include public communications but preferably subject to no loss (or very limited loss) of SKC-DoF.

Specifically, in Section II, we will present a generalized channel probing (GCP) method for a multiple-input and multiple-output (MIMO) scattering-rich wireless (or wireline discussed later) channel between Alice and Bob against multiple-antenna Eve where Alice, Bob and Eve have n_A, n_B and n_E antennas respectively. For the GCP, we let both Alice and Bob transmit random sequences of vectors with durations m_A and m_B respectively in each channel coherence period, which leads to the data sets $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$ at Alice, Bob and Eve for each channel coherence period. We will show that the DoF of the SKC C_S based on $\{\mathcal{X}, \mathcal{Y}, \mathcal{Z}\}$ is

$$DoF(C_S) = \min(n_B, (n_A - n_E)^+)(m_A - n_A) + \min(n_A, (n_B - n_E)^+)(m_B - n_B) + n_A n_B \delta_{|\rho|-1} \quad (1)$$

where $\delta_{|\rho|-1} = 1$ if the MIMO channel is (perfectly) reciprocal, and $\delta_{|\rho|-1} = 0$ otherwise. The precise definition of $\delta_{|\rho|-1}$ along with other assumptions will be given in the discussions leading to Theorem 1. The proof of Theorem 1 is provided in Sections III, IV, V and VI.

Furthermore, in Section VII, we will present a generalized pre-processing (GPP) method. Assuming $n_B \leq n_A$, GPP allows public communications, from Bob to Alice (and to Eve), of a random matrix $\mathbf{U}$ superimposed onto $\mathcal{Y}$, which consequently allows Alice to obtain a consistent estimate $\hat{\mathbf{U}}$ of $\mathbf{U}$. Because of the public communications, the data sets available at Alice, Bob and Eve after GPP are changed to the new sets $\mathcal{X}'$, $\mathcal{Y}'$ and $\mathcal{Z}'$. We will show that the DoF of the SKC C'_S based on $\mathcal{X}'$, $\mathcal{Y}'$ and $\mathcal{Z}'$ is also given by (1). See Theorem 2. With fully randomized transmissions from Alice and Bob during GCP, the computation required during GPP to exploit the channel reciprocity is nontrivial. Additional constraints on $\mathbf{U}$ can be useful to reduce the computational complexity but potentially at a slight loss of SKC-DoF as shown in Corollaries 1 and 2. In Section VIII, we show the Cramer-Rao lower bound for the estimation task at Alice during GPP. In Section IX, we show the proof of Theorem 2 and Corollaries 1 and 2.

In Section X, we consider the situation where parts of the random transmissions from Alice and Bob during GCP are made public. Interestingly, as shown in Theorem 3, there is still no loss of SKC-DoF from that given by (1). The public pilots from Alice and Bob allow them to estimate their reciprocal channel matrix, which can naturally be used to contribute the term $n_A n_B \delta_{|\rho|-1}$ in (1). The other transmissions from Alice and Bob during GCP can be also used rather efficiently during GPP to yield the other terms in (1). Such a simple GPP scheme is discussed in Section XII where Theorem 4 provides the sufficient and necessary condition on any specific realization of the legitimate and eavesdropping channel matrices in order for the scheme to achieve a positive SKC-DoF, assuming that Eve has the full knowledge of all channel matrices and there is no channel reciprocity.

The most important contributions in this paper are Theorems 1, 2, 3 and 4. The other sections and materials in this paper provide the necessary details to support and/or complement those contributions. Note that despite varying complexities of several versions of GCP and GPP shown in this paper, they can be all used to achieve the SKC-DoF shown in (1).

Notations: Vectors and matrices are denoted by boldface lower cases and boldface upper cases respectively. Unless defined otherwise, $\mathbf{x} = vec(\mathbf{X})$ and $\mathbf{x}_t = vec(\mathbf{X}^T)$ where $vec(\mathbf{X})$ vertically stacks all columns of the matrix $\mathbf{X}$ into the column vector $\mathbf{x}$. A set of any kind of elements is denoted by calligraphic upper case or by $\{\cdot\}$. The set of all $n \times m$ complex matrices is $\mathcal{C}^{n\times m}$. The mutual information between $\mathcal{A}$ and $\mathcal{B}$ conditioned on $\mathcal{C}$ is $I(\mathcal{A}; \mathcal{B}|\mathcal{C})$. The differential entropy of a random matrix $\mathbf{X}$ conditioned on another random matrix $\mathbf{Y}$ is $h(\mathbf{X}|\mathbf{Y})$. The probability density function (PDF) of a circular complex Gaussian random vector with mean $\mathbf{m}$ and covariance matrix $\mathbf{R}$ is $\mathcal{CN}(\mathbf{m}, \mathbf{R})$. The expectation operator is $\mathbb{E}$. The real and imaginary parts of $\mathbf{X}$ are $\Re(\mathbf{X})$ and $\Im(\mathbf{X})$. The determinant of matrix $\mathbf{X}$ is $|\mathbf{X}|$. The vector from column-wise stacking of matrix $\mathbf{X}$ is $vec(\mathbf{X})$. The Kronecker product between $\mathbf{X}$ and $\mathbf{Y}$ is $\mathbf{X} \otimes \mathbf{Y}$. $(x)^+ = \max(0, x)$. Logarithm with base 2 is log, and logarithm with base e is ln. Transpose, conjugate, conjugate transpose and pseudoinverse are the superscripts ^{T}, *, ^{H} and † respectively. The non-superscript $*$ denotes a quantity of no importance. $range(\mathbf{X})$, $row(\mathbf{X})$ and $null(\mathbf{X})$ denote respectively the column span, row span and right null space of $\mathbf{X}$. Also $\doteq$, $\in$, $\subset$ and $\not\subset$ denote "defined as," "belongs to," "subset of (or same set as)" and "not subset of (or not same set as)". Other notations are defined in context.

II. Generalized Channel Probing

Consider a MIMO flat-fading channel between node A (Alice) and node B (Bob) with n_A and n_B antennas respectively. In the broadband case, this flat-fading channel may correspond to a subcarrier in an orthogonal frequency division multiplexing

(OFDM) system. Let node A transmit the $n_A \times m_A$ matrix $\mathbf{X}_A$ over $m_A \geq n_A$ time slots, and node B transmit the $n_B \times m_B$ matrix $\mathbf{X}_B$ over another $m_B \geq n_B$ time slots. Then the signals received by node A and node B are respectively

$$\mathbf{Y}_A = \mathbf{H}_{A,B}\mathbf{X}_B + \mathbf{W}_A, \in \mathcal{C}^{n_A \times m_B}, \tag{2}$$

$$\mathbf{Y}_B = \mathbf{H}_{B,A}\mathbf{X}_A + \mathbf{W}_B, \in \mathcal{C}^{n_B \times m_A}, \tag{3}$$

and the signals received by Eve (with n_E antennas) are both of the following matrices:

$$\mathbf{Y}_{E,A} = \mathbf{G}_A\mathbf{X}_A + \mathbf{W}_{E,A}, \in \mathcal{C}^{n_E \times m_A}, \tag{4}$$

$$\mathbf{Y}_{E,B} = \mathbf{G}_B\mathbf{X}_B + \mathbf{W}_{E,B}, \in \mathcal{C}^{n_E \times m_B}. \tag{5}$$

Here $\mathbf{H}_{A,B}$ is the channel matrix from node B to node A, $\mathbf{G}_A$ is the channel matrix from node A to Eve, and $\mathbf{H}_{B,A}$ and $\mathbf{G}_B$ are similarly defined. The noise terms are represented by the $\mathbf{W}$ matrices. Also note that for digital radio communication, a public pilot is generally required for carrier-frequency and/or carrier-phase synchronization. But such a pilot can be transmitted via a separate subcarrier in an OFDM system or via an auxiliary antenna, e.g., see [11], [12]. For the antennas and subcarrier under consideration here, we assume that no public pilot is necessary.

After the channel probing, the data sets available at node A, node B and Eve are respectively $\mathcal{X} = \{\mathbf{X}_A, \mathbf{Y}_A\}$, $\mathcal{Y} = \{\mathbf{X}_B, \mathbf{Y}_B\}$, and $\mathcal{Z} = \{\mathbf{Y}_{E,A}, \mathbf{Y}_{E,B}\}$. We will be interested in the degree of freedom (DoF) of the secret key capacity based on $\{\mathcal{X}, \mathcal{Y}, \mathcal{Z}\}$. We will also be interested in a pre-processing by which Alice and Bob produce a pair of highly correlated secret vectors based on $\{\mathcal{X}, \mathcal{Y}, \mathcal{Z}\}$ and further transmission via a public channel. The pair of secret vectors should be ready for secret key generation via established methods of quantization, reconciliation and privacy amplification. Furthermore, we will be interested in how much, if any, the pre-processing incurs a loss of DoF from that based on $\{\mathcal{X}, \mathcal{Y}, \mathcal{Z}\}$.

It is clear that channel probing does not require any coding and can be done with a high spectral efficiency within each channel coherence period. Differing from transmission of a secret from one node to another over the MIMO channel, a secret key based on $\{\mathcal{X}, \mathcal{Y}, \mathcal{Z}\}$ can be generated by Alice and Bob via public communications over any other (public or private) channel after they have established $\mathcal{X}$ and $\mathcal{Y}$ respectively from the probed MIMO channel.

For DoF analysis, we assume the following. All entries in $\mathbf{X}_A$ and $\mathbf{X}_B$ are independent and identically distributed (i.i.d.) with the PDF $\mathcal{CN}(0, P)$. All entries in $\mathbf{W}_A$, $\mathbf{W}_B$, $\mathbf{W}_{E,A}$ and $\mathbf{W}_{E,B}$ are i.i.d. $\mathcal{CN}(0, 1)$. All entries in $\mathbf{G}_A$ and $\mathbf{G}_B$ are i.i.d. $\mathcal{CN}(0, \sigma_g^2)$ where σ_g^2 remains comparable to one when $P \to \infty$. All entries in each of $\mathbf{H}_{A,B}$ and $\mathbf{H}_{B,A}$ are i.i.d. $\mathcal{CN}(0, 1)$. $vec(\mathbf{H}_{A,B})$ and $vec(\mathbf{H}_{B,A}^T)$ are jointly Gaussian with the correlation matrix $\rho\mathbf{I}_{n_An_B}$. If $|\rho| = 1$, the channel between nodes A and B is said to be (perfectly) reciprocal. If $|\rho| < 1$, the channel is said to be not reciprocal. Unless already mentioned otherwise, the above matrices are independent of each other.

Note that P is proportional to the transmission power. For DoF analysis, we will assume a large P or $P \to \infty$.

Lemma 1: Given the above described model of $\{\mathcal{X}, \mathcal{Y}, \mathcal{Z}\}$, the secret key capacity C_S in bits per independent realization of $\{\mathcal{X}, \mathcal{Y}, \mathcal{Z}\}$ is bounded as follows:

$$C_L \leq C_S \leq C_U \tag{6}$$

with $C_L = I(\mathcal{X};\mathcal{Y}) - \min(I(\mathcal{X};\mathcal{Z}), I(\mathcal{Y};\mathcal{Z}))$, and $C_U = \min(I(\mathcal{X};\mathcal{Y}), I(\mathcal{X};\mathcal{Y}|\mathcal{Z}))$.

Proof: This lemma follows from an argument of the master definition of mutual information shown in [19] and Theorem 4.1 in [17] for discrete and memoryless $\{\mathcal{X}, \mathcal{Y}, \mathcal{Z}\}$, the latter of which is also available in [18]. ■

We will also write $C_L = \max(C_A, C_B)$ with $C_A = I(\mathcal{X};\mathcal{Y}) - I(\mathcal{X};\mathcal{Z})$ and $C_B = I(\mathcal{X};\mathcal{Y}) - I(\mathcal{Y};\mathcal{Z})$, or equivalently $C_A = h(\mathcal{X}|\mathcal{Z}) - h(\mathcal{X}|\mathcal{Y})$ and $C_B = h(\mathcal{Y}|\mathcal{Z}) - h(\mathcal{Y}|\mathcal{X})$. And $C_U \leq C_Z$ with $C_Z = I(\mathcal{X};\mathcal{Y}|\mathcal{Z}) = h(\mathcal{X}|\mathcal{Z}) - h(\mathcal{X}|\mathcal{Y},\mathcal{Z})$.

It should be noted that finding an easy-to-compute or even easy-to-simulate expression of C_L with no loss of DoF (or C_U with no increase of DoF) for the current problem for an arbitrary $\{n_A, n_B, n_E\}$ seems an unsolved challenge. A key reason is the products of Gaussian distributed matrices in (2)–(5). In this paper, our focus is on the DoF of C_L and C_U subject to given scheme of channel probing and/or pre-processing.

Theorem 1: If $n_A \geq n_B$, then $DoF(C_B) = DoF(C_L) = DoF(C_S) = DoF(C_U) = DoF(C_Z)$. And for all (n_A, n_B),

$$DoF(C_S) = a_{A,B} + a_{B,A} + b_{A,B} + b_{B,A} - 2n_An_B + n_An_B\delta_{|\rho|-1} \tag{7}$$

where $a_{A,B} = \min(n_B, (n_A - n_E)^+)m_A$, $b_{A,B} = \min(n_B, (n_B + n_E - n_A)^+)n_A$, $\delta_{|\rho|-1} = 0$ if $|\rho| < 1$, and $\delta_{|\rho|-1} = 1$ if $|\rho| = 1$. Note that (7) is equivalent to (1) as shown by (133).

Proof: The proof is given in Sections III, IV, V and VI. ■

A. Discussion of $DoF(C_S)$

1) For $n_E \geq \max(n_A, n_B)$: In this case, (7) reduces to

$$DoF(C_S) = n_An_B\delta_{|\rho|-1} \tag{8}$$

which is zero if $|\rho| < 1$, or n_An_B if $|\rho| = 1$. In [4], the case of $n_A = n_B = 1$ was considered. The above result shows that their channel probing scheme with $m_A \geq 1$ and/or $m_B \geq 1$ has the same DoF (which is one) as using $m_A = m_B = 1$.

2) For $n_B \leq N_e < n_A$: In this case, (7) reduces to

$$DoF(C_S) = \min(n_B, (n_A - n_E)^+)m_A + (n_B + n_E - n_A)^+n_A - n_An_B + n_An_B\delta_{|\rho|-1} \tag{9}$$

which increases as m_A ($\geq n_A$) increases, but is invariant to m_B ($\geq n_B$). Also in this case, the channel reciprocity is not necessary for a positive or even large DoF. The above result is useful for such situation where a base station with a large number of antennas needs to establish a secret key with a mobile node with a small number of antennas.

In [5], a channel probing scheme was proposed for a multi-antenna Alice and a single-antenna Bob. In their scheme, Alice transmits random symbols via randomly selected antennas sequentially. We show in Section XI that the DoF of SKC of their scheme subject to the reciprocal channel condition between Alice and Bob is only n_A for each independent subcarrier and independent coherence period even if Eve has a smaller number of antennas than Alice (i.e., for all $n_E \geq 1$).

The special case (9) also has a connection with the result shown in [14] where the authors considered a notion called secret-key diversity multiplexing tradeoff (DMT). Based on the data sets resulting from transmissions from Alice to Bob (and to Eve) and a secret-key-rate outage probability at high SNR, they showed that the DMT is equivalent to that of a

MIMO channel with $n_A - n_E$ transmit antennas and n_B receive antennas. This implies that the maximum multiplexity gain of their SKG scheme is $\min(n_B, (n_A - n_E)^+)$, which coincides with the coefficient of m_A in (9). In Section XII, we will discuss a related case where Alice transmits random symbols via the MIMO channel and Bob uses a public channel to send secret information superimposed onto the signals received from Alice.

3) For $n_E < \min(n_A, n_B)$: In this case, (7) reduces to

$$DoF(C_S) = \min(n_B, (n_A - n_E)^+)m_A + \min(n_A, (n_B - n_E)^+)m_B + n_A n_B \delta_{|\rho|-1} \tag{10}$$

which increases as either m_A or m_B increases. The first term corresponds to the transmission from node A to node B while the second term to the transmission from node B to node A.

4) Comparison to Wiretap Channel Model: Theorem 1 is based on what is called source model for physical layer security [17]. In [13], a MIMO wiretap-channel (WTC) model is considered where secret information is directly transmitted over the channel without additional public communications. Using the notations defined in this paper, the main conclusion from [13] is that the DoF of the secrecy capacity $C_{S,WTC}$ for direct transmission over the $n_A \times n_B$ MIMO channel against Eve with n_E antennas in bits per channel coherent period of total T sampling intervals is

$$DoF(C_{S,WTC}) = (\min(n_A, n_B) - n_E)^+ (T - \min(n_A, n_B)) \tag{11}$$

provided $T \geq 2\min(n_A, n_B)$.

We see that $DoF(C_{S,WTC})$ does not benefit from a possible reciprocity of the channel, and $DoF(C_{S,WTC})$ vanishes as soon as $n_E \geq \min(n_A, n_B)$. None of these is the case for $DoF(C_S)$. As shown in (9), for $n_B \leq n_E < n_A$, $DoF(C_S)$ increases with m_A. For the case of $n_E < \min(n_A, n_B)$, we can let $n_A \geq n_B$ and $T = m_A + m_B$, then we see

$$\begin{aligned} &DoF(C_S) - DoF(C_{S,WTC}) \\ &= (\min[n_B, (n_A - n_E)] - (n_B - n_E))m_A \\ &\quad + (n_B - n_E)n_B + n_A n_B \delta_{|\rho|-1}. \end{aligned} \tag{12}$$

The above is strictly positive and also increases with m_A subject to $n_A > n_B$. This observation should have important practical implications in regard to "direct transmission of a secret key or information over the channel" versus "generation of a secret key from the channel assisted by public communications over another channel".

5) Using Public Pilots and Random Symbols: It will be shown in Section X that if n_A columns of $\mathbf{X}_A$ and n_B columns of $\mathbf{X}_B$ are publicly known, there is no loss of DoF of C_S from that given by (7). The term $n_A n_B \delta_{|\rho|-1}$ in (7) can be achieved via reciprocal channel estimation based on the public pilots, and the other terms in (7) are due to the random symbols in $\mathbf{X}_A$ and $\mathbf{X}_B$.

6) Optimal m_A and m_B: It is important to note that $m_A + m_B$ is in theory upper bounded by the product T of the coherence time and the coherence bandwidth of the MIMO channel. If $n_A > n_B$ and we want to exploit the channel reciprocity, then the optimal m_A and m_B that maximize $DoF(C_S)$ are $m_A = T - m_B$ and $m_B = n_B$. If there is no channel reciprocity, then the optimal m_A and m_B are $m_A = T$ and $m_B = 0$. In Section XII, we will discuss the special case of GCP and GPP with $m_A > n_A$ and $m_B = 0$.

III. Analysis of $h(\mathcal{X}|\mathcal{Y})$

In this section, we will present all the necessary details to obtain the DoF of $h(\mathcal{X}|\mathcal{Y})$. One of the important results that are also useful for later sections is (27).

We know

$$\begin{aligned} h(\mathcal{X}|\mathcal{Y}) &= h(\mathbf{X}_A, \mathbf{Y}_A|\mathbf{X}_B, \mathbf{Y}_B) \\ &= h(\mathbf{X}_A|\mathbf{X}_B, \mathbf{Y}_B) + h(\mathbf{Y}_A|\mathbf{X}_A, \mathbf{X}_B, \mathbf{Y}_B) \\ &= h(\mathbf{X}_A|\mathbf{Y}_B) + h(\mathbf{Y}_A|\mathbf{X}_A, \mathbf{X}_B, \mathbf{Y}_B) \end{aligned} \tag{13}$$

where for the last equality we have applied that $\mathbf{X}_B$ is independent of $\{\mathbf{X}_A, \mathbf{Y}_B\}$. Now we write

$$h(\mathbf{X}_A|\mathbf{Y}_B) = h(\mathbf{X}_A) + h(\mathbf{Y}_B|\mathbf{X}_A) - h(\mathbf{Y}_B). \tag{14}$$

Since $\mathbf{x}_A = vec(\mathbf{X}_A)$ has the PDF $\mathcal{CN}(0, (P+1)\mathbf{I}_{n_A m_A})$, we have $h(\mathbf{X}_A) = \log((\pi e)^{n_A m_A}|(P+1)\mathbf{I}_{n_A m_A}|) = n_A m_A \log(\pi e(P+1))$ and hence

$$DoF(h(\mathbf{X}_A)) = n_A m_A. \tag{15}$$

To consider $h(\mathbf{Y}_B|\mathbf{X}_A)$ in (14), let $\mathbf{y}_B = vec(\mathbf{Y}_B)$. Also define other similar notations of vectors accordingly. Then it follows from (3) that $\mathbf{y}_B = (\mathbf{X}_A^T \otimes \mathbf{I}_{n_B})\mathbf{h}_{B,A} + \mathbf{w}_B$ and equivalently $\mathbf{y}_B = (\mathbf{I}_{m_A} \otimes \mathbf{H}_{B,A})\mathbf{x}_A + \mathbf{w}_B$. Given $\mathbf{X}_A$, $\mathbf{y}_B$ has the PDF $\mathcal{CN}(0, \mathbf{R}_{\mathbf{y}_B|\mathbf{x}_A})$ with $\mathbf{R}_{\mathbf{y}_B|\mathbf{x}_A} = \mathbf{X}_A^T\mathbf{X}_A^* \otimes \mathbf{I}_{n_B} + \mathbf{I}_{n_B m_A}$. Then

$$\begin{aligned} h(\mathbf{Y}_B|\mathbf{X}_A) &= \mathbb{E}\{\log((\pi e)^{n_B m_A}|\mathbf{R}_{\mathbf{y}_B|\mathbf{x}_A}|)\} \\ &= n_B \mathbb{E}\{\log((\pi e)^{m_A}|\mathbf{X}_A^T\mathbf{X}_A^* + \mathbf{I}_{m_A}|)\}. \end{aligned} \tag{16}$$

Since $rank(\mathbf{X}_A) = n_A$ due to $n_A \leq m_A$, we have

$$DoF(h(\mathbf{Y}_B|\mathbf{X}_A)) = n_A n_B. \tag{17}$$

A. Analysis of $h(\mathbf{Y}_B)$

For $h(\mathbf{Y}_B)$ in (14), we consider the two cases "$n_B \leq n_A$" and "$n_B > n_A$" separately.

1) $h(\mathbf{Y}_B)$ for $n_B \leq n_A$: For $n_B \leq n_A$, we consider the following lower and upper bounds on $h(\mathbf{Y}_B)$: $h(\mathbf{Y}_B|\mathbf{H}_{B,A}) \leq h(\mathbf{Y}_B) \leq h(\mathbf{Y}'_B)$ where $\mathbf{y}'_B$ is so defined that it has the PDF $\mathcal{CN}(0, \mathbf{R}_{\mathbf{y}_B})$ with

$$\mathbf{R}_{\mathbf{y}_B} = \mathbb{E}\{\mathbf{y}_B\mathbf{y}_B^H\} = \mathbb{E}\{\mathbf{R}_{\mathbf{y}_B|\mathbf{x}_A}\} = (n_A P + 1)\mathbf{I}_{n_B m_A}. \tag{18}$$

It follows that $h(\mathbf{Y}'_B) = \log((\pi e)^{n_B m_A}|\mathbf{R}_{\mathbf{y}_B}|)$ and hence

$$DoF(h(\mathbf{Y}'_B)) = n_B m_A. \tag{19}$$

Given $\mathbf{H}_{B,A}$, $\mathbf{y}_B$ has the PDF $\mathcal{CN}(0, \mathbf{R}_{\mathbf{y}_B|\mathbf{H}_{B,A}})$ with $\mathbf{R}_{\mathbf{y}_B|\mathbf{H}_{B,A}} = P(\mathbf{I}_{m_A} \otimes \mathbf{H}_{B,A}\mathbf{H}_{B,A}^H) + \mathbf{I}_{n_B m_A}$. Hence, $h(\mathbf{Y}_B|\mathbf{H}_{B,A}) = \mathbb{E}\{\log((\pi e)^{n_B m_A}|\mathbf{R}_{\mathbf{y}_B|\mathbf{H}_{B,A}}|)\}$ and then

$$DoF(h(\mathbf{Y}_B|\mathbf{H}_{B,A})) = n_B m_A. \tag{20}$$

Since (19) and (20) (the upper and lower bounds on $DoF(h(\mathbf{Y}_B))$) coincide, we have

$$DoF(h(\mathbf{Y}_B)) = n_B m_A. \tag{21}$$

2) $h(\mathbf{Y}_B)$ for $n_B > n_A$: For $n_B > n_A$, we let $\mathbf{Y}_B^T = [\mathbf{Y}_{B,1}^T, \mathbf{Y}_{B,2}^T]$ where $\mathbf{Y}_{B,1}$ consists of the first n_A rows of $\mathbf{Y}_B$ and $\mathbf{Y}_{B,2}$ consists of the last $n_B - n_A$ rows of $\mathbf{Y}_B$. It follows that $\mathbf{Y}_{B,1} = \mathbf{H}_{B,A,1}\mathbf{X}_A + \mathbf{W}_{B,1}$ and $\mathbf{Y}_{B,2} = \mathbf{H}_{B,A,2}\mathbf{X}_A + \mathbf{W}_{B,2}$ where the additional notations are defined in an obvious way. It then follows that $h(\mathbf{Y}_B) = h(\mathbf{Y}_{B,1}) + h(\mathbf{Y}_{B,2}|\mathbf{Y}_{B,1})$. Similar to (21), we have

$$DoF(h(\mathbf{Y}_{B,1})) = n_A m_A. \tag{22}$$

To consider $h(\mathbf{Y}_{B,2}|\mathbf{Y}_{B,1})$, we first write $h(\mathbf{Y}_{B,2}|\mathbf{Y}_{B,1}) \approx h(\mathbf{Y}_{B,2}|\mathbf{H}_{B,A,1}\mathbf{X}_A) \geq h(\mathbf{Y}_{B,2}|\mathbf{H}_{B,A,1}\mathbf{X}_A, \mathbf{H}_{B,A,1}) = h(\mathbf{Y}_{B,2}|\mathbf{X}_A)$ where the approximation holds at high power without affecting the DoF. Since $\mathbf{y}_{B,2} = (\mathbf{X}_A^T \otimes \mathbf{I}_{n_B - n_A})\mathbf{h}_{B,A,2} + \mathbf{w}_{B,2}$, $\mathbf{y}_{B,2}$ given $\mathbf{X}_A$ has the PDF $\mathcal{CN}(0, \mathbf{R}_{\mathbf{y}_{B,2}|\mathbf{x}_A})$ with $\mathbf{R}_{\mathbf{y}_{B,2}|\mathbf{x}_A} = (\mathbf{X}_A^T\mathbf{X}_A^* \otimes \mathbf{I}_{n_B - n_A}) + \mathbf{I}_{(n_B - n_A)m_A}$. Hence, $h(\mathbf{Y}_{B,2}|\mathbf{X}_A) = \mathbb{E}\{\log((\pi e)^{(n_B - n_A)m_A}|\mathbf{R}_{\mathbf{y}_{B,2}|\mathbf{x}_A}|)\}$. Since $rank(\mathbf{X}_A) = n_A$, we have

$$DoF(h(\mathbf{Y}_{B,2}|\mathbf{Y}_{B,1})) \geq DoF(h(\mathbf{Y}_{B,2}|\mathbf{X}_A)) = n_A(n_B - n_A). \tag{23}$$

Now let us write the QR decomposition of $\mathbf{H}_{B,A,1}\mathbf{X}_A$ as $\mathbf{H}_{B,A,1}\mathbf{X}_A = \mathbf{R}_1\mathbf{Q}_1$ where $\mathbf{Q}_1$ is a $n_A \times m_A$ row-wise orthonormal matrix. Since the row span of $\mathbf{H}_{B,A,2}\mathbf{X}_A$ belongs to the row span of $\mathbf{X}_A$ or equivalently of $\mathbf{Q}_1$, it follows that there exists $(n_B - n_A)n_A$ matrix $\mathbf{R}_2$ such that $\mathbf{H}_{B,A,2}\mathbf{X}_A = \mathbf{R}_2\mathbf{Q}_1$. Since $\mathbf{Q}_1$ is a function of $\mathbf{H}_{B,A,1}\mathbf{X}_A$, we have $h(\mathbf{Y}_{B,2}|\mathbf{Y}_{B,1}) \approx h(\mathbf{Y}_{B,2}|\mathbf{H}_{B,A,1}\mathbf{X}_A) \leq h(\mathbf{Y}_{B,2}|\mathbf{Q}_1)$. Since $\mathbf{y}_{B,A,2} = (\mathbf{Q}_1^T \otimes \mathbf{I}_{n_B - n_A})\mathbf{r}_2 + \mathbf{w}_{B,A,2}$, we have $h(\mathbf{Y}_{B,2}|\mathbf{Q}_1) \leq \mathbb{E}\{\log((\pi e)^{(n_B - n_A)n_A}|\mathbf{R}_{\mathbf{y}_{B,A,2}|\mathbf{Q}_1}|)\}$ where $\mathbf{R}_{\mathbf{y}_{B,A,2}|\mathbf{Q}_1} = (\mathbf{Q}_1^T \otimes \mathbf{I}_{n_B - n_A})\mathbf{R}_{\mathbf{r}_2}(\mathbf{Q}_1^* \otimes \mathbf{I}_{n_B - n_A}) + \mathbf{I}_{(n_B - n_A)n_A}$. It is obvious that $DoF(h(\mathbf{Y}_{B,2}|\mathbf{Q}_1)) \leq (n_B - n_A)n_A$ and hence

$$DoF(h(\mathbf{Y}_{B,2}|\mathbf{Y}_{B,1})) \leq (n_B - n_A)n_A. \tag{24}$$

Since the upper bound in (24) agrees with the lower bound in (23), we have

$$DoF(h(\mathbf{Y}_{B,2}|\mathbf{Y}_{B,1})) = (n_B - n_A)n_A. \tag{25}$$

Combining (25) with (22), we have

$$DoF(h(\mathbf{Y}_B)) = n_A m_A + (n_B - n_A)n_A. \tag{26}$$

3) $h(\mathbf{Y}_B)$ for Any n_A and n_B: Combining the above results (21) and (26) for the cases of $n_B \leq n_A$ and $n_B > n_A$ respectively, we have

$$DoF(h(\mathbf{Y}_B)) = \min(n_A, n_B)m_A + (n_B - n_A)^+ n_A. \tag{27}$$

Clearly, $DoF(h(\mathbf{Y}_A))$ when needed is also given by the above but with "A" and "B" exchanged.

We can also translate (27) into a general lemma:

Lemma 2: If $\mathbf{Y} = \mathbf{H}\mathbf{X} + \mathbf{W}$ where $\mathbf{H}$ is an $l \times n$ matrix consisting of i.i.d. $\mathcal{CN}(0,1)$ elements, $\mathbf{X}$ is an $n \times m$ matrix consisting of i.i.d. $\mathcal{CN}(0, P)$ elements, and $\mathbf{W}$ is an $l \times m$ matrix consisting of i.i.d. $\mathcal{CN}(0,1)$ elements, then relative to P, for $m \geq n$,

$$DoF(h(\mathbf{Y})) = \min(l, n)m + (l - n)^+ n. \tag{28}$$

B. Analysis of $h(\mathbf{X}_A|\mathbf{Y}_B)$ and $h(\mathbf{Y}_A|\mathbf{X}_A, \mathbf{X}_B, \mathbf{Y}_B)$

It follows from (14), (15), (17) and (27) that

$$\begin{aligned} &DoF(h(\mathbf{X}_A|\mathbf{Y}_B)) \\ &= n_A n_B + n_A m_A - \min(n_A, n_B)m_A - (n_B - n_A)^+ n_A \\ &= \min(n_A, n_B)n_A + (n_A - n_B)^+ m_A. \end{aligned} \tag{29}$$

Now we consider $h(\mathbf{Y}_A|\mathbf{X}_A, \mathbf{X}_B, \mathbf{Y}_B)$ in (13), which can be written at a high power as $h(\mathbf{Y}_A|\mathbf{X}_A, \mathbf{X}_B, \mathbf{Y}_B) \approx h(\mathbf{Y}_A|\mathbf{X}_B, \mathbf{H}_{B,A})$. Recall $\mathbf{y}_A = (\mathbf{X}_B^T \otimes \mathbf{I}_{n_A})\mathbf{h}_{A,B} + \mathbf{w}_A$. Given $\{\mathbf{X}_B, \mathbf{H}_{B,A}\}$, $\mathbf{y}_A$ has the PDF $\mathcal{CN}(\mathbf{m}_{\mathbf{h}_{A,B}|\mathbf{h}_{B,A}}, \mathbf{R}_{\Delta\mathbf{h}_{A,B}|\mathbf{h}_{B,A}})$ with $\mathbf{m}_{\mathbf{h}_{A,B}|\mathbf{h}_{B,A}} = \mathbb{E}\{\mathbf{h}_{A,B}|\mathbf{h}_{B,A}\}$ and $\mathbf{R}_{\Delta\mathbf{h}_{A,B}|\mathbf{h}_{B,A}} = (1 - |\rho|^2)(\mathbf{X}_B^T\mathbf{X}_B^* \otimes \mathbf{I}_{n_A}) + \mathbf{I}_{n_A m_B}$. Hence $h(\mathbf{Y}_A|\mathbf{X}_B, \mathbf{H}_{B,A}) = \mathbb{E}\{\log((\pi e)^{n_A m_B}|\mathbf{R}_{\Delta\mathbf{h}_{A,B}|\mathbf{h}_{B,A}}|)\}$. Since $rank(\mathbf{X}_B) = n_B$, we now have

$$\begin{aligned} DoF(h(\mathbf{Y}_A|\mathbf{X}_A, \mathbf{X}_B, \mathbf{Y}_B)) &= DoF(h(\mathbf{Y}_A|\mathbf{X}_B, \mathbf{H}_{B,A})) \\ &= n_A n_B(1 - \delta_{|\rho|-1}). \end{aligned} \tag{30}$$

C. Result

It follows from (13), (29) and (30) that

$$\begin{aligned} DoF(h(\mathcal{X}|\mathcal{Y})) = &\min(n_A, n_B)n_A + (n_A - n_B)^+ m_A \\ &+ n_A n_B(1 - \delta_{|\rho|-1}). \end{aligned} \tag{31}$$

Note that $DoF(h(\mathcal{Y}|\mathcal{X}))$ follows by symmetry from that of $DoF(h(\mathcal{X}|\mathcal{Y}))$ by exchanging "A" and "B".

IV. Analysis of $h(\mathcal{X}|\mathcal{Z})$

In this section, we will derive the DoF of $h(\mathcal{X}|\mathcal{Z})$. We can write

$$\begin{aligned} h(\mathcal{X}|\mathcal{Z}) &= h(\mathbf{X}_A|\mathcal{Z}) + h(\mathbf{Y}_A|\mathbf{X}_A, \mathcal{Z}) \\ &= h(\mathbf{X}_A|\mathbf{Y}_{E,A}, \mathbf{Y}_{E,B}) + h(\mathbf{Y}_A|\mathbf{X}_A, \mathbf{Y}_{E,A}, \mathbf{Y}_{E,B}) \\ &= h(\mathbf{X}_A|\mathbf{Y}_{E,A}) + h(\mathbf{Y}_A|\mathbf{Y}_{E,B}) \end{aligned} \tag{32}$$

where in the last equation we have applied that $\mathbf{Y}_{E,B}$ is independent of $\{\mathbf{X}_A, \mathbf{Y}_{E,A}\}$, and $\{\mathbf{X}_A, \mathbf{Y}_{E,A}\}$ is independent of $\{\mathbf{Y}_A, \mathbf{Y}_{E,B}\}$.

A. Analysis of $h(\mathbf{X}_A|\mathbf{Y}_{E,A})$

To consider $h(\mathbf{X}_A|\mathbf{Y}_{E,A})$ in (32), we write

$$h(\mathbf{X}_A|\mathbf{Y}_{E,A}) = h(\mathbf{Y}_{E,A}|\mathbf{X}_A) + h(\mathbf{X}_A) - h(\mathbf{Y}_{E,A}). \tag{33}$$

Note that $\mathbf{y}_{E,A} = (\mathbf{X}_A^T \otimes \mathbf{I}_{n_E})\mathbf{g}_A + \mathbf{w}_{E,A}$. So, $\mathbf{y}_{E,A}$ given $\mathbf{X}_A$ has the PDF $\mathcal{CN}(0, \mathbf{R}_{\mathbf{y}_{E,A}|\mathbf{x}_A})$ with $\mathbf{R}_{\mathbf{y}_{E,A}|\mathbf{x}_A} = \sigma_g^2(\mathbf{X}_A^T\mathbf{X}_A^* \otimes \mathbf{I}_{n_E}) + \mathbf{I}_{n_E m_A}$. Hence $h(\mathbf{Y}_{E,A}|\mathbf{X}_A) = \mathbb{E}\{\log((\pi e)^{n_E m_A}|\mathbf{R}_{\mathbf{y}_{E,A}|\mathbf{x}_A}|)\}$. Since $rank(\mathbf{X}_A) = n_A$, we have

$$DoF(h(\mathbf{Y}_{E,A}|\mathbf{X}_A)) = n_E n_A. \tag{34}$$

Following a similar analysis as that for $DoF(h(\mathbf{Y}_B))$ in (27), we have

$$DoF(h(\mathbf{Y}_{E,A})) = \min(n_A, n_E)m_A + (n_E - n_A)^+ n_A. \tag{35}$$

It follows from (33), (15), (34) and (35) that

$$\begin{aligned} &DoF(h(\mathbf{X}_A|\mathbf{Y}_{E,A})) \\ &= n_A m_A + n_E n_A - \min(n_A, n_E)m_A - (n_E - n_A)^+ n_A \\ &= (n_A - n_E)^+ m_A + \min(n_A, n_E)n_A. \end{aligned} \tag{36}$$

B. Analysis of $h(\mathbf{Y}_A|\mathbf{Y}_{E,B})$

To consider $h(\mathbf{Y}_A|\mathbf{Y}_{E,B})$ in (32), we write

$$h(\mathbf{Y}_A|\mathbf{Y}_{E,B}) = h(\mathbf{Y}_A, \mathbf{Y}_{E,B}) - h(\mathbf{Y}_{E,B}). \tag{37}$$

Following a similar analysis as that for $DoF(h(\mathbf{Y}_B))$ in (27), we have

$$DoF(h(\mathbf{Y}_{E,B})) = \min(n_B, n_E)m_B + (n_E - n_B)^+ n_B, \tag{38}$$

$$DoF(h(\mathbf{Y}_A, \mathbf{Y}_{E,B})) = \min(n_B, n_A + n_E)m_B + (n_A + n_E - n_B)^+ n_B. \tag{39}$$

Note that $\{\mathbf{Y}_A, \mathbf{Y}_{E,B}\}$ can be written as

$$\begin{bmatrix} \mathbf{Y}_A \\ \mathbf{Y}_{E,B} \end{bmatrix} = \begin{bmatrix} \mathbf{H}_{A,B} \\ \mathbf{G}_B \end{bmatrix} \mathbf{X}_B + \begin{bmatrix} \mathbf{W}_A \\ \mathbf{W}_{E,B} \end{bmatrix} \tag{40}$$

where the left side can be viewed as the signals received by $n_A + n_E$ antennas over m_B time slots in response to the signal matrix $\mathbf{X}_B$ transmitted by node B. The fact that σ_q^2 may be not equal to one has little effect on the analysis. Taking the difference between (37) and (39) yields

$$DoF(h(\mathbf{Y}_A|\mathbf{Y}_{E,B})) = \min(n_A, (n_B - n_E)^+)m_B + \min(n_A, (n_A + n_E - n_B)^+)n_B. \tag{41}$$

C. Result

It follows from (32), (36) and (41) that

$$DoF(h(\mathcal{X}|\mathcal{Z})) = (n_A - n_E)^+ m_A + \min(n_A, n_E)n_A + \min(n_A, (n_B - n_E)^+)m_B + \min(n_A, (n_A + n_E - n_B)^+)n_B. \tag{42}$$

Note that $DoF(h(\mathcal{Y}|\mathcal{Z}))$ follows by symmetry from that of $DoF(h(\mathcal{X}|\mathcal{Z}))$ by exchanging "A" and "B".

V. Analysis of $h(\mathcal{X}|\mathcal{Y}, \mathcal{Z})$

In this section, we will derive the DoF of $h(\mathcal{X}|\mathcal{Y}, \mathcal{Z})$. Using the components in $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$, we can write $h(\mathcal{X}|\mathcal{Y}, \mathcal{Z}) = h(\mathbf{X}_A|\mathcal{Y}, \mathcal{Z}) + h(\mathbf{Y}_A|\mathbf{X}_A, \mathcal{Y}, \mathcal{Z}) = h(\mathbf{X}_A|\mathbf{X}_B, \mathbf{Y}_B, \mathbf{Y}_{E,A}, \mathbf{Y}_{E,B}) + h(\mathbf{Y}_A|\mathbf{X}_A, \mathbf{X}_B, \mathbf{Y}_B, \mathbf{Y}_{E,A}, \mathbf{Y}_{E,B})$ and hence

$$h(\mathcal{X}|\mathcal{Y}, \mathcal{Z}) = h(\mathbf{X}_A|\mathbf{Y}_B, \mathbf{Y}_{E,A}) + h(\mathbf{Y}_A|\mathbf{X}_A, \mathbf{X}_B, \mathbf{Y}_B) \tag{43}$$

where we have used the fact that $\{\mathbf{X}_B, \mathbf{Y}_{E,B}\}$ is independent of $\{\mathbf{X}_A, \mathbf{Y}_B, \mathbf{Y}_{E,A}\}$ and the fact that given $\{\mathbf{X}_A, \mathbf{X}_B\}$, $\{\mathbf{Y}_{E,A}, \mathbf{Y}_{E,B}\}$ is independent of $\{\mathbf{Y}_A, \mathbf{Y}_B\}$. The DoF of the second term in (43) is already shown in (30). Next we only need to focus on the first term.

A. Analysis of $h(\mathbf{X}_A|\mathbf{Y}_B, \mathbf{Y}_{E,A})$

We can write

$$h(\mathbf{X}_A|\mathbf{Y}_B, \mathbf{Y}_{E,A}) = h(\mathbf{Y}_B, \mathbf{Y}_{E,A}|\mathbf{X}_A) + h(\mathbf{X}_A) - h(\mathbf{Y}_B, \mathbf{Y}_{E,A}). \tag{44}$$

Similar to (34) and (39) respectively, we have

$$DoF(h(\mathbf{Y}_B, \mathbf{Y}_{E,A}|\mathbf{X}_A)) = (n_B + n_E)n_A, \tag{45}$$

$$DoF(h(\mathbf{Y}_B, \mathbf{Y}_{E,A})) = \min(n_A, n_B + n_E)m_A + (n_B + n_E - n_A)^+ n_A. \tag{46}$$

It follows from (15),(44), (45) and (46) that

$$DoF(h(\mathbf{X}_A|\mathbf{Y}_B, \mathbf{Y}_{E,A})) = (n_A - n_B - n_E)^+ m_A + \min(n_A, n_B + n_E)n_A. \tag{47}$$

B. Result

It follows from (43), (30) and (47) that

$$DoF(h(\mathcal{X}|\mathcal{Y}, \mathcal{Z})) = n_A n_B(1 - \delta_{|\rho|-1}) + (n_A - n_B - n_E)^+ m_A + \min(n_A, n_B + n_E)n_A. \tag{48}$$

VI. Degree of Freedom of C_S

Given (31), (42) and (48), both of the followings are readily available:

$$DoF(C_A) = DoF(h(\mathcal{X}|\mathcal{Z})) - DoF(h(\mathcal{X}|\mathcal{Y})), \tag{49}$$

$$DoF(C_Z) = DoF(h(\mathcal{X}|\mathcal{Z})) - DoF(h(\mathcal{X}|\mathcal{Y}, \mathcal{Z})). \tag{50}$$

We also have $DoF(C_B) = DoF(h(\mathcal{Y}|\mathcal{Z})) - DoF(h(\mathcal{Y}|\mathcal{X}))$, which is the same as $DoF(C_A)$ after exchanging "A" and "B".

A gap between the upper and lower bounds of $DoF(C_S)$ is

$$\begin{aligned} &DoF(C_Z) - DoF(C_A) \\ &= DoF(h(\mathcal{X}|\mathcal{Y})) - DoF(h(\mathcal{X}|\mathcal{Y}, \mathcal{Z})) \\ &= \min(n_A, n_B)n_A + (n_A - n_B)^+ m_A \\ &\quad - (n_A - n_B - n_E)^+ m_A - \min(n_A, n_B + n_E)n_A \\ &= \min(n_E, (n_A - n_B)^+)(m_A - n_A) \end{aligned} \tag{51}$$

where the 2nd equality follows from (31) and (48), and the 3rd equality follows from the fact that both $(n_A - n_B)^+ - (n_A - n_B - n_E)^+$ and $\min(n_A, n_B + n_E) - \min(n_A, n_B)$ equal to $\min(n_E, (n_A - n_B)^+)$.

We see that if $n_A \le n_B$, $DoF(C_Z) - DoF(C_A) = 0$. Note that C_Z is invariant to the exchange of "A" and "B". Hence, if $n_B \le n_A$, $DoF(C_Z) - DoF(C_B) = 0$. Therefore, $DoF(C_Z) = \max(DoF(C_A), DoF(C_B))$ for all (n_A, n_B), and hence $DoF(C_S) = DoF(C_Z)$ for all (n_A, n_B).

Also note that C_A is the secrecy capacity based on a one-way public transmission scheme from node A to node B after $\{\mathcal{X}, \mathcal{Y}, \mathcal{Z}\}$ is given, and C_B is that from node B to node A. See page 120 of [17]. So, if $n_A \ge n_B$, then a one-way public transmission scheme from node B to node A can achieve the DoF of C_S, which is the inspiration for the GPP proposed later in Section VII.

Using (42) and (48) in (50) does not directly result in a form that is obviously invariant to the exchange of "A" and "B". To obtain an explicit expression of $DoF(C_Z)$ that is obviously invariant to the exchange, let us recall

$$\begin{aligned} C_Z &= I(\mathcal{X}; \mathcal{Y}|\mathcal{Z}) \\ &= h(\mathcal{X}|\mathcal{Z}) - h(\mathcal{X}|\mathcal{Y}, \mathcal{Z}) \\ &= h(\mathbf{X}_A|\mathbf{Y}_{E,A}, \mathbf{Y}_{E,B}) + h(\mathbf{Y}_A|\mathbf{X}_A, \mathbf{Y}_{E,A}, \mathbf{Y}_{E,B}) \end{aligned}$$

$$
\begin{aligned}
&- h(\mathbf{X}_A|\mathbf{X}_B, \mathbf{Y}_B, \mathbf{Y}_{E,A}, \mathbf{Y}_{E,B}) \\
&- h(\mathbf{Y}_A|\mathbf{X}_A, \mathbf{X}_B, \mathbf{Y}_B, \mathbf{Y}_{E,A}, \mathbf{Y}_{E,B}) \\
&= h(\mathbf{X}_A|\mathbf{Y}_{E,A}) + h(\mathbf{Y}_A|\mathbf{Y}_{E,B}) - h(\mathbf{X}_A|\mathbf{Y}_B, \mathbf{Y}_{E,A}) \\
&\quad - h(\mathbf{Y}_A|\mathbf{X}_A, \mathbf{X}_B, \mathbf{Y}_B) \\
&= h(\mathbf{Y}_{E,A}|\mathbf{X}_A) + h(\mathbf{X}_A) - h(\mathbf{Y}_{E,A}) + h(\mathbf{Y}_A, \mathbf{Y}_{E,B}) \\
&\quad - h(\mathbf{Y}_{E,B}) - h(\mathbf{Y}_B, \mathbf{Y}_{E,A}|\mathbf{X}_A) - h(\mathbf{X}_A) + h(\mathbf{Y}_B, \mathbf{Y}_{E,A}) \\
&\quad - h(\mathbf{Y}_A|\mathbf{X}_A, \mathbf{X}_B, \mathbf{Y}_B) \\
&= [h(\mathbf{Y}_A, \mathbf{Y}_{E,B}) + h(\mathbf{Y}_B, \mathbf{Y}_{E,A})] - [h(\mathbf{Y}_{E,A}) + h(\mathbf{Y}_{E,B})] \\
&\quad - [h(\mathbf{Y}_B, \mathbf{Y}_{E,A}|\mathbf{X}_A) - h(\mathbf{Y}_{E,A}|\mathbf{X}_A)] \\
&\quad - h(\mathbf{Y}_A|\mathbf{X}_A, \mathbf{X}_B, \mathbf{Y}_B). \qquad (52)
\end{aligned}
$$

Then, applying (39), (46), (35), (38), (45), (34) and (30) to the corresponding seven terms in (52), we have

$$
\begin{aligned}
&DoF(C_Z) = DoF(C_S) \\
&= \min(n_B, n_A + n_E)m_B + (n_A + n_E - n_B)^+ n_B \\
&\quad + \min(n_A, n_B + n_E)m_A + (n_B + n_E - n_A)^+ n_A \\
&\quad - \min(n_A, n_E)m_A - (n_E - n_A)^+ n_A - \min(n_B, n_E)m_B \\
&\quad - (n_E - n_B)^+ n_B - n_A n_B - n_A n_B(1 - \delta_{|\rho|-1}). \qquad (53)
\end{aligned}
$$

The above expression is clearly invariant to the exchange of "A" and "B". Furthermore, (53) can be simplified to (7).

VII. Generalized Pre-Processing

Now we present a generalized pre-processing (GPP) method for SKG based on the observations by Alice, Bob and Eve shown in (2)–(5) where there is no public pilot. We will assume $n_A \geq n_B$.

First let us recall a property of the mutual information $I(\mathcal{X}; \mathcal{Y})$:

$$
\begin{aligned}
&I(\mathcal{X}; \mathcal{Y}) = h(\mathcal{X}) - h(\mathcal{X}|\mathcal{Y}) \\
&= h(\mathbf{X}_A) + h(\mathbf{Y}_A) - h(\mathbf{X}_A|\mathbf{Y}_B) - h(\mathbf{Y}_A|\mathbf{X}_A, \mathbf{X}_B, \mathbf{Y}_B) \\
&= h(\mathbf{Y}_A) + h(\mathbf{Y}_B) - h(\mathbf{Y}_B|\mathbf{X}_A) - h(\mathbf{Y}_A|\mathbf{X}_A, \mathbf{X}_B, \mathbf{Y}_B). \qquad (54)
\end{aligned}
$$

Applying (27), (17) and (30) to the above, one can verify that

$$
\begin{aligned}
&DoF(I(\mathcal{X}; \mathcal{Y}) \\
&= \begin{cases} n_B(m_A + m_B - n_B), & \mathbf{H}_{A,B} = \mathbf{H}_{B,A}^T, \\ n_B(m_A + m_B - n_A - n_B), & \mathbf{H}_{A,B} \neq \mathbf{H}_{B,A}^T. \end{cases} \qquad (55)
\end{aligned}
$$

Note that a pre-processing method aims to generate a pair of secret vectors at Alice and Bob that are ready to be quantized into a pair of bit streams which can be then further processed by reconciliation and privacy amplification. Any leakage to Eve during channel probing, pre-processing and any other steps will need to (and can) be taken care of during privacy amplification. Furthermore, it is desirable that the pair of secret vectors generated by preprocessing on the raw data $\{\mathcal{X}, \mathcal{Y}\}$ preserves the DoF of $I(\mathcal{X}; \mathcal{Y})$ given by (55). It is also desirable that any leakage to Eve during pre-processing does not reduce the DoF of the secret key capacity from that given by (7).

We will next primarily consider the reciprocal channel case where $\mathbf{H}_{A,B} = \mathbf{H}_{B,A}^T = \mathbf{H}$. For the non-reciprocal channel case where $\mathbf{H}_{A,B} \neq \mathbf{H}_{B,A}^T$, a discussion is given later in Section VII-C.

Our proposed GPP for the reciprocal channel case is as follows. Bob first generates a complex-valued random matrix $\mathbf{U} = [\mathbf{U}_0, \mathbf{U}_1, \mathbf{U}_2]$ where the submatrices have the dimensions $n_B \times n_B$, $n_B \times (m_A - n_B)$ and $n_B \times (m_B - n_B)$ respectively. Notice that the total number of complex elements in $\mathbf{U}$ equals $DoF(I(\mathcal{X}; \mathcal{Y}))$. We will further assume that the entries in $\mathbf{U}$ are i.i.d. $\mathcal{CN}(0, P')$ where P' is comparable to P or simply $P' = P$. Then the DoF of $h(\mathbf{U})$ equals $DoF(I(\mathcal{X}; \mathcal{Y}))$ in (55) for the reciprocal channel case. And if Alice can obtain a consistent estimate $\hat{\mathbf{U}}$ of $\mathbf{U}$, then Alice and Bob have a pair of secret vectors, i.e., $vec(\hat{\mathbf{U}})$ and $vec(\mathbf{U})$, whose mutual information has the same DoF as $I(\mathcal{X}; \mathcal{Y})$.

Then, in order for Alice to be able to estimate $\mathbf{U}$, Bob performs an "incoming signal assisted transmission (iSAT)," i.e., he sends out $\mathbf{X}'_B = \mathbf{X}_B + [\mathbf{U}_0, \mathbf{U}_2]$ and $\mathbf{Y}'_B = \mathbf{Y}_B + [\mathbf{U}_0, \mathbf{U}_1]$ via any reliable public channel to Alice. Here we assume that both Alice and Eve receive $\mathbf{X}'_B$ and $\mathbf{Y}'_B$ with a negligible noise compared to $\mathbf{W}_A$ and $\mathbf{W}_B$.

Theorem 2: Let $\mathcal{X}' = \{\mathcal{X}, \mathbf{X}'_B, \mathbf{Y}'_B\}$, $\mathcal{Y}' = \{\mathcal{Y}, \mathbf{U}\}$ and $\mathcal{Z}' = \{\mathcal{Z}, \mathbf{X}'_B, \mathbf{Y}'_B\}$. Then, for $n_A \geq n_B$, the secret key capacity C'_S based on $\{\mathcal{X}', \mathcal{Y}', \mathcal{Z}'\}$ has the same DoF as C_S based on $\{\mathcal{X}, \mathcal{Y}, \mathcal{Z}\}$, i.e.,

$$DoF(C'_S) = DoF(C_S). \qquad (56)$$

Proof: The proof is given in Section IX. ■

This theorem says that the leakage to Eve due to $\{\mathbf{X}'_B, \mathbf{Y}'_B\}$ does not change the DoF of the secret key capacity from that given by (7). The GPP is inspired by a conceptual approach shown in Section 4.2.1 in [17] where Bob transmits publicly the modulo sum of a uniform random variable $\mathcal{U}$ and a discrete $\mathcal{Y}$ (both belong to a common finite set). By doing so, the lower bound C_B on C_S is achieved. But an application of that approach for $\{\mathcal{X}, \mathcal{Y}, \mathcal{Z}\}$ given in this paper would require (among major issues) a proper coding scheme, which is not yet available.

A. Estimation of $\mathbf{U}$ by Alice

To show how Alice can estimate $\mathbf{U}$, notice the key equations that Alice now has:

$$\mathbf{Y}_A = \mathbf{H}(\mathbf{X}'_B - [\mathbf{U}_0, \mathbf{U}_2]) + \mathbf{W}_A, \qquad (57)$$

$$\mathbf{Y}'_B = \mathbf{H}^T\mathbf{X}_A + [\mathbf{U}_0, \mathbf{U}_1] + \mathbf{W}_B, \qquad (58)$$

where the unknowns are $\mathbf{H}$ and $\mathbf{U} = [\mathbf{U}_0, \mathbf{U}_1, \mathbf{U}_2]$. Also notice that (57) is nonlinear. To show more insights into (57) and (58), we let $\mathbf{Y}_A = [\mathbf{Y}_{A,\alpha}, \mathbf{Y}_{A,\beta}]$ with $\mathbf{Y}_{A,\alpha}$ consisting of the first n_B columns of $\mathbf{Y}_A$ and $\mathbf{Y}_{A,\beta}$ consisting of all other columns of $\mathbf{Y}_A$. We will use the subscripts $_\alpha$ and $_\beta$ to indicate the same partitions for all relevant matrices. Then we know

$$\mathbf{Y}_{A,\alpha} = \mathbf{H}[\mathbf{X}'_{B,\alpha} - \mathbf{U}_0] + \mathbf{W}_{A,\alpha}, \qquad (59)$$

$$\mathbf{Y}_{A,\beta} = \mathbf{H}[\mathbf{X}'_{B,\beta} - \mathbf{U}_2] + \mathbf{W}_{A,\beta}, \qquad (60)$$

$$\mathbf{Y}'_{B,\alpha} = \mathbf{H}^T\mathbf{X}_{A,\alpha} + \mathbf{U}_0 + \mathbf{W}_{B,\alpha}, \qquad (61)$$

$$\mathbf{Y}'_{B,\beta} = \mathbf{H}^T\mathbf{X}_{A,\beta} + \mathbf{U}_1 + \mathbf{W}_{B,\beta}. \qquad (62)$$

If $\hat{\mathbf{H}}$ is given, then the least-square (LS) estimates of $\mathbf{U}_0$, $\mathbf{U}_1$ and $\mathbf{U}_2$ are as follows:

$$\hat{\mathbf{U}}_0 = (\hat{\mathbf{H}}^H\hat{\mathbf{H}} + \mathbf{I}_{n_B})^{-1}(-\hat{\mathbf{H}}^H\Delta\mathbf{Y}_{A,\alpha} + \Delta\mathbf{Y}'_{B,\alpha}), \qquad (63)$$

$$\hat{\mathbf{U}}_1 = \mathbf{Y}'_{B,\beta} - \hat{\mathbf{H}}^T \mathbf{X}_{A,\beta}, \tag{64}$$

$$\hat{\mathbf{U}}_2 = -(\hat{\mathbf{H}}^H \hat{\mathbf{H}})^{-1} \hat{\mathbf{H}}^H \Delta\mathbf{Y}_{A,\beta}, \tag{65}$$

with $\Delta\mathbf{Y}_{A,\alpha} = \mathbf{Y}_{A,\alpha} - \hat{\mathbf{H}}\mathbf{X}'_{B,\alpha}$, $\Delta\mathbf{Y}'_{B,\alpha} = \mathbf{Y}'_{B,\alpha} - \hat{\mathbf{H}}^T\mathbf{X}_{A,\alpha}$ and $\Delta\mathbf{Y}_{A,\beta} = \mathbf{Y}_{A,\beta} - \hat{\mathbf{H}}\mathbf{X}'_{B,\beta}$. Note that (63) is the LS solution of $\mathbf{U}_0$ to (59) and (61), or equivalently,

$$\hat{\mathbf{U}}_0 = arg \min_{\mathbf{U}_0} J_0 \tag{66}$$

with

$$J_0 = \left\| \begin{bmatrix} \Delta\mathbf{Y}_{A,\alpha} \\ \Delta\mathbf{Y}'_{B,\alpha} \end{bmatrix} - \begin{bmatrix} -\hat{\mathbf{H}} \\ \mathbf{I}_{n_B} \end{bmatrix} \mathbf{U}_0 \right\|_F^2. \tag{67}$$

Here $\|\mathbf{M}\|_F^2 \doteq Tr(\mathbf{M}\mathbf{M}^H)$ for any matrix $\mathbf{M}$. We will also write $J_0 = \|\mathbf{Y}_0 - \mathbf{H}_0\mathbf{U}_0\|_F^2$ with $\mathbf{Y}_0$ and $\mathbf{H}_0$ defined in an obvious way.

If $\hat{\mathbf{U}}_0$ is a consistent estimate of $\mathbf{U}_0$, then a consistent estimate of $\mathbf{H}$ follows from (59), i.e.,

$$\hat{\mathbf{H}} = \mathbf{Y}_{A,\alpha}[\mathbf{X}'_{B,\alpha} - \hat{\mathbf{U}}_0]^{-1} \tag{68}$$

which then leads to consistent estimates of $\mathbf{U}_1$ and $\mathbf{U}_2$ via (64) and (65).

To find a consistent estimate $\hat{\mathbf{U}}_0$, we can use (68) in (61), which yields

$$(\mathbf{X}'_{B,\alpha} - \hat{\mathbf{U}}_0)^T(\mathbf{Y}'_{B,\alpha} - \hat{\mathbf{U}}_0) = \mathbf{Y}_{A,\alpha}^T\mathbf{X}_{A,\alpha}. \tag{69}$$

This is an $n_B \times n_B$ quadratic matrix equation of the $n_B \times n_B$ unknown matrix $\hat{\mathbf{U}}_0$, which in general have multiple (but no more than $2^{n_B^2}$) solutions. One of the solutions in the absence of noise is the desired solution $\mathbf{U}_0$.

Every solution to (69) can be written as $\hat{\mathbf{U}}_0 = \mathbf{U}_0 - \Delta\hat{\mathbf{U}}_0$. Then (69) implies $(\mathbf{X}_{B,\alpha} + \Delta\hat{\mathbf{U}}_0)^T(\mathbf{Y}_{B,\alpha} + \Delta\hat{\mathbf{U}}_0) = \mathbf{Y}_{A,\alpha}^T\mathbf{X}_{A,\alpha}$. Clearly, every nonzero $\Delta\hat{\mathbf{U}}_0$ in the absence of noise is independent of $\mathbf{U}_0$. For example, if $n_B = 1$, then $\Delta\hat{\mathbf{U}}_0 = -\mathbf{X}_{B,\alpha} - \mathbf{Y}_{B,\alpha}$. Furthermore, one can verify that the corresponding estimates of $\mathbf{U}_1$ and $\mathbf{U}_2$ from (64) and (65) can be also written as $\hat{\mathbf{U}}_1 = \mathbf{U}_1 - \Delta\hat{\mathbf{U}}_1$ and $\hat{\mathbf{U}}_2 = \mathbf{U}_2 - \Delta\hat{\mathbf{U}}_2$ where $\Delta\hat{\mathbf{U}}_1$ and $\Delta\hat{\mathbf{U}}_2$ in the absence of noise are also independent of $\mathbf{U}$. Therefore, among all solutions to (69) in the absence of noise, the desired solution has the minimum variance. Provided that the number $n_U = n_B(m_A + m_B - n_B)$ of entries in $\mathbf{U}$ is large, the desired solution to (69) can be detected by choosing the one corresponding to the smallest $\frac{1}{Pn_U}\|\hat{\mathbf{U}}\|_F^2$ which approaches to one for large n_U.

Alternatively, the desired solution to (69) can be detected if there is an additional constraint on $\mathbf{U}_0$. For example, Bob informs Alice, via public channel, of $\mathbf{C}$ and d such that

$$Tr(\mathbf{C}^T\mathbf{U}_0) = d. \tag{70}$$

Corollary 1: For the reciprocal channel case, i.e., $|\rho| = 1$, if there is the public constraint (70), then there is a loss of one DoF in the secret key capacity from that given by (7) with $\delta_{|\rho|-1} = 1$.

Proof: See Section IX. ■

With a good initial $\hat{\mathbf{U}}_0$, there is a good initial $\hat{\mathbf{H}}$ from (68). Also note that for any given $\hat{\mathbf{H}}$, the optimal estimate of $\mathbf{U}_0$ subject to (70) has a closed form as shown next. The Lagrangian function of this problem is

$$L_0 = J_0 + \mu_r \Re(Tr(\mathbf{C}^T\mathbf{U}_0) - d) + \mu_i \Im(Tr(\mathbf{C}^T\mathbf{U}_0) - d) \tag{71}$$

where μ_r and μ_i are two real-valued multipliers. One can verify that $\frac{\partial L_0}{\partial \mathbf{U}_0} \doteq \frac{\partial L_0}{\partial \Re(\mathbf{U}_0)} + j\frac{\partial L_0}{\partial \Im(\mathbf{U}_0)} = -2\mathbf{H}_0^H(\mathbf{Y}_0 - \mathbf{H}_0\mathbf{U}_0) + \mu\mathbf{C}^*$ with $\mu = \mu_r + j\mu_i$. Then the solution of $\mathbf{U}_0$ to $\frac{\partial L_0}{\partial \mathbf{U}_0} = 0$ is

$$\hat{\mathbf{U}}_0 = (\mathbf{H}_0^H\mathbf{H}_0)^{-1}\left(\mathbf{H}_0^H\mathbf{Y}_0 - \frac{\mu}{2}\mathbf{C}^*\right). \tag{72}$$

Applying (70), we have

$$\frac{\mu}{2} = \frac{Tr(\mathbf{C}^T(\mathbf{H}_0^H\mathbf{H}_0)^{-1}\mathbf{Y}_0 - d)}{Tr(\mathbf{C}^T(\mathbf{H}_0^H\mathbf{H}_0)^{-1}\mathbf{C}^*)}. \tag{73}$$

Note that (72)–(73) is the LS estimate of $\mathbf{U}_0$ subject to a fixed $\hat{\mathbf{H}}$ and (70), and this estimate reduces to (63) if (70) is absent or equivalently $\mu = 0$.

1) Maximum Likelihood Estimation: To find the maximum likelihood (ML) estimates of all unknowns (i.e., $\mathbf{H}$, $\mathbf{U}_0$, $\mathbf{U}_1$ and $\mathbf{U}_2$), we need to find the unknowns that minimize the following cost function:

$$J = \|\mathbf{Y}_A - \mathbf{H}(\mathbf{X}'_B - [\mathbf{U}_0, \mathbf{U}_2])\|_F^2 + \|\mathbf{Y}'_B - \mathbf{H}^T\mathbf{X}_A - [\mathbf{U}_0, \mathbf{U}_1]\|_F^2. \tag{74}$$

We already know that if $\hat{\mathbf{H}}$ is the ML estimate (or equivalently the LS estimate) of $\mathbf{H}$, then the ML estimates of $\mathbf{U}_0$, $\mathbf{U}_1$ and $\mathbf{U}_2$ are available in closed forms as shown before.

To find the ML estimate of $\mathbf{H}$ subject to a good initial estimate $\hat{\mathbf{H}}^{(0)}$, we can use the gradient method as follows:

$$\hat{\mathbf{H}}^{(k+1)} = \hat{\mathbf{H}}^{(k)} - \eta \left.\frac{\partial J}{\partial \mathbf{H}}\right|_k \tag{75}$$

where k denotes the k-th iteration, and η is a step size. Furthermore, one can verify from (74) that

$$\frac{\partial J}{\partial \mathbf{H}} = -2(\mathbf{Y}_A - \mathbf{H}(\mathbf{X}'_B - [\mathbf{U}_0, \mathbf{U}_2]))(\mathbf{X}'_B - [\mathbf{U}_0, \mathbf{U}_2])^H - 2[(\mathbf{Y}'_B - \mathbf{H}^T\mathbf{X}_A - [\mathbf{U}_0, \mathbf{U}_1])\mathbf{X}_A^H]^T \tag{76}$$

where $\mathbf{H}$, $\mathbf{U}_0$, $\mathbf{U}_1$ and $\mathbf{U}_2$ need to be replaced by their best estimates at every iteration.

Upon convergence of the gradient algorithm, the final estimate $\hat{\mathbf{U}}$ of $\mathbf{U}$ at Alice should be highly correlated with $\mathbf{U}$ originally generated by Bob. As the power P increases, $\frac{1}{P}\|\hat{\mathbf{U}} - \mathbf{U}\|_F^2$ decreases to zero. The variances of the entries in $\hat{\mathbf{U}}$ at large P can be measured by the Cramer-Rao lower bound as discussed in Section VIII.

B. Discussion

1) Extracting a Common Vector by Reciprocal Multiplication: Since Alice knows $\mathbf{X}_A$ and $\mathbf{Y}_A = \mathbf{H}_{A,B}\mathbf{X}_B + \mathbf{W}_A$ or equivalently $\mathbf{y}_A = vec(\mathbf{Y}_A) = (\mathbf{X}_B^T \otimes \mathbf{I}_{n_A})\mathbf{h}_{A,B} + \mathbf{w}_A$, she can compute

$$\mathbf{z}_A \doteq (\mathbf{I}_{m_B} \otimes \mathbf{X}_A^T)\mathbf{y}_A = (\mathbf{X}_B^T \otimes \mathbf{X}_A^T)\mathbf{h}_{A,B} + (\mathbf{I}_{m_B} \otimes \mathbf{X}_A^T)\mathbf{w}_A. \tag{77}$$

Similarly, Bob knows $\mathbf{X}_B$ and $\mathbf{Y}_B = \mathbf{H}_{B,A}\mathbf{X}_A + \mathbf{W}_B$ or equivalently $\mathbf{y}_{B,t} = vec(\mathbf{Y}_B^T) = (\mathbf{I}_{n_B} \otimes \mathbf{X}_A^T)\mathbf{h}_{A,B} + \mathbf{w}_{B,t}$, and he can compute

$$\mathbf{z}_B \doteq (\mathbf{X}_B^T \otimes \mathbf{I}_{m_A})\mathbf{y}_{B,t} = (\mathbf{X}_B^T \otimes \mathbf{X}_A^T)\mathbf{h}_{A,B} + (\mathbf{X}_B^T \otimes \mathbf{I}_{m_A})\mathbf{w}_{B,t}. \quad (78)$$

The multiplications performed on $\mathbf{y}_A$ and $\mathbf{y}_{B,t}$ respectively in (77) and (78) can be referred to as reciprocal multiplications. It is clear that at high power, both $\mathbf{z}_A$ and $\mathbf{z}_B$ are dominated by the common vector $\mathbf{v} \doteq (\mathbf{X}_B^T \otimes \mathbf{X}_A^T)\mathbf{h}_{A,B}$. Therefore, it follows that $DoF(h(\mathbf{z}_A|\mathbf{z}_B)) = 0$ and hence

$$DoF(I(\mathbf{z}_A;\mathbf{z}_B)) = DoF(h(\mathbf{z}_A)) = DoF(h(\mathbf{v})). \quad (79)$$

It is easy to verify that $\mathbb{E}\{\mathbf{v}\mathbf{v}^H\} = Pn_B\mathbf{I}_{m_B} \otimes Pn_A\mathbf{I}_{m_A} = n_An_BP^2\mathbf{I}_{m_Am_B}$, which implies that the entries in $\mathbf{v}$ are all pair-wise uncorrelated. But the entries in $\mathbf{v}$ are non-Gaussian, and in general they are not statistically independent of each other.

Since $\mathbf{z}_A$ and $\mathbf{z}_B$ are functions of $\mathcal{X}$ and $\mathcal{Y}$ respectively, we have $I(\mathbf{z}_A;\mathbf{z}_B) \le I(\mathcal{X};\mathcal{Y})$ and from (79) and (55) that

$$DoF(h(\mathbf{v})) \le n_B(m_A + m_B - n_B). \quad (80)$$

Since $\mathbf{v}$ has the dimension $m_Am_B \times 1$ and $m_Am_B \ge n_B(m_A + m_B - n_B)$ (due to $m_A \ge n_A \ge n_B$ and $m_B \ge n_B$), there is generally statistical dependence among the entries in $\mathbf{v}$.

For example, consider the case of $n_A = n_B = 1$ and $m_A = m_B = 2$. Then we can write $\mathbf{X}_A = [a_1, a_2]$, $\mathbf{X}_B = [b_1, b_2]$ and $\mathbf{H}_{A,B} = [h]$. Hence

$$\mathbf{v} = [v_1, v_2, v_3, v_4]^T = [b_1a_1h, b_1a_2h, b_2a_1h, b_2a_2h]^T. \quad (81)$$

One can verify that v_4 is uniquely determined by v_1, v_2 and v_3, i.e., $v_4 = \frac{v_2v_3}{v_1}$. At the same time, we see that $\mathbb{E}\{\mathbf{v}\mathbf{v}^H\} = P^2\mathbf{I}_4$, i.e., the 4 entries in $\mathbf{v}$ are pair-wise uncorrelated.

2) A Special Case: For $n_A = n_B = 1$ and $m_A = m_B = m$, we let $\mathbf{X}_A^T = \mathbf{a}$, $\mathbf{X}_B^T = \mathbf{b}$, $\mathbf{Y}_A^T = \mathbf{y}_A$, $\mathbf{Y}_B^T = \mathbf{y}_B$. For this case, the authors of [4] proposed the following strategy where Alice and Bob compute respectively $\mathbf{z}'_A \doteq \mathbf{a} \odot \mathbf{y}_A$ and $\mathbf{z}'_B \doteq \mathbf{b} \odot \mathbf{y}_B$ where $\odot$ denotes the element-wise product. At high power, $\mathbf{z}'_A$ and $\mathbf{z}'_B$ share the common vector $\mathbf{v}' = (\mathbf{a} \odot \mathbf{b})h$ which has the dimension m. In this case, it follows that

$$DoF(I(\mathbf{z}'_A;\mathbf{z}'_B)) = m \quad (82)$$

which is however smaller than the corresponding $DoF(I(\mathcal{X};\mathcal{Y})) = 2m - 1$ for $m > 1$.

C. The Case of $|\rho| < 1$ or $\mathbf{H}_{A,B} \ne \mathbf{H}_{B,A}^T$

For this non-reciprocal channel case, we see from (55) that the DoF of $I(\mathcal{X};\mathcal{Y})$ is reduced by n_An_B. In this case, we can let $\mathbf{U}_0$ and the first $n_A - n_B$ columns of $\mathbf{U}_1$ be public, and then the remaining entries in $\mathbf{U}$ have the DoF equal to $DoF(I(\mathcal{X};\mathcal{Y}))$ given by (55) for the non-reciprocal channel case.

One can verify that with $\mathcal{X}$, $\mathbf{X}'_B$ and $\mathbf{Y}'_B$, Alice can obtain consistent estimates of all non-public entries in $\mathbf{U}$. Specifically, Alice can compute an initial consistent estimate of $\mathbf{H}_{A,B}$ based on (59) as follows: $\hat{\mathbf{H}}_{A,B} = \mathbf{Y}_{A,\alpha}(\mathbf{X}'_{B,\alpha} - \mathbf{U}_0)^{-1}$. With any $\hat{\mathbf{H}}_{A,B}$, the ML estimate of $\mathbf{U}_2$ is the LS solution of (60), i.e.,

$$\hat{\mathbf{U}}_2 = \mathbf{X}'_{B,\beta} - (\hat{\mathbf{H}}_{A,B}^H\hat{\mathbf{H}}_{A,B})^{-1}\hat{\mathbf{H}}_{A,B}^H\mathbf{Y}_{A,\beta}. \quad (83)$$

The ML estimate of $\mathbf{H}_{A,B}$ (and hence $\mathbf{U}_2$) can be found by a gradient search of the LS solution of (59) and (60) with $\mathbf{H} = \mathbf{H}_{A,B}$, i.e., $\hat{\mathbf{H}}_{A,B,k+1} = \hat{\mathbf{H}}_{A,B,k} - \eta\frac{\partial J_1}{\partial \mathbf{H}_{A,B}}\Big|_k$ where J_1 is the first term in (74), and $\frac{\partial J_1}{\partial \mathbf{H}_{A,B}}$ is the first term in (76) with $\mathbf{H} = \mathbf{H}_{A,B}$. For ML estimation of $\mathbf{H}_{B,A}$ and the unknowns in $\mathbf{U}_1$, let $\mathbf{Y}'_{B,\gamma}$ and $\mathbf{X}_{A,\gamma}$ be each the first n_A columns of $\mathbf{Y}'_B$ and $\mathbf{X}_A$ respectively, $\mathbf{U}_\gamma$ be the first n_A columns of $[\mathbf{U}_0, \mathbf{U}_1]$, and $\mathbf{U}_\tau$, $\mathbf{Y}'_{B,\tau}$ and $\mathbf{X}_{A,\tau}$ be each the last $m_A - n_A$ columns of $\mathbf{U}_1$, $\mathbf{Y}'_B$ and $\mathbf{X}_A$ respectively. Then the ML estimates of $\mathbf{H}_{B,A}$ and $\mathbf{U}_\tau$ are given by the LS solution to (61) and (62) with $\mathbf{H}^T = \mathbf{H}_{B,A}$, i.e.,

$$[\hat{\mathbf{H}}_{B,A}, \hat{\mathbf{U}}_\tau] = [\mathbf{T}_1, \mathbf{Y}'_{B,\tau}]\begin{bmatrix}\mathbf{X}_A\mathbf{X}_A^H & \mathbf{X}_{A,\tau} \\ \mathbf{X}_{A,\tau}^H & \mathbf{I}_{m_A-n_A}\end{bmatrix}^{-1} \quad (84)$$

with $\mathbf{T}_1 = (\mathbf{Y}'_{B,\gamma} - \mathbf{U}_\gamma)\mathbf{X}_{A,\gamma}^H + \mathbf{Y}'_{B,\tau}\mathbf{X}_{A,\tau}^H$.

Note that unlike the case where a reciprocal channel is fully exploited, the complexity of the above method is much lower. Furthermore, if we know that $n_A > n_E \ge n_B$, then the optimal choice of m_B in terms of SKC-DoF can be chosen to be n_B as discussed in Section II-A2. In this case, $\mathbf{U}_2$ is empty, and the estimation of $\mathbf{H}_{A,B}$ is no longer needed. In other words, if $m_B = n_B$, Alice only needs the optimal estimate of the $n_B \times (m_A - n_A)$ matrix $\mathbf{U}_\tau$ as given in (84), which can be further written (using block matrix inversion) as

$$\hat{\mathbf{U}}_\tau = \mathbf{T}_1\mathbf{T}_2 + \mathbf{Y}'_{B,\tau}\mathbf{T}_3 \quad (85)$$

with $\mathbf{T}_2 = -(\mathbf{X}_{A,\gamma}\mathbf{X}_{A,\gamma}^H)^{-1}\mathbf{X}_{A,\tau}$ and $\mathbf{T}_3 = \mathbf{I}_{m_A-n_A} + \mathbf{X}_{A,\tau}^H(\mathbf{X}_{A,\gamma}\mathbf{X}_{A,\gamma}^H)^{-1}\mathbf{X}_{A,\tau}$. (The MMSE estimate of $\mathbf{U}_\tau$ could also be used by Alice, which is however not to be discussed.) Alice and Bob can then use the pair of secret vectors $vec(\hat{\mathbf{U}}_\tau)$ and $vec(\mathbf{U}_\tau)$, respectively, to generate the final secret key.

Corollary 2: For the non-reciprocal channel case, i.e., $|\rho| < 1$, if $\mathbf{U}_0$ and the first (or any) $n_A - n_B$ columns of $\mathbf{U}_1$ are public, then there is no loss of DoF in the secret key capacity from that given by (7) with $\delta_{|\rho|-1} = 0$.

Proof: See Section IX. ■

VIII. Cramer-Rao Lower Bound

In this section, we show the Cramer-Rao lower bound (CRLB) for the covariance matrix of the estimates of all unknowns by Alice during GPP. Since CRLB is for unbiased estimates, it is generally a lower bound achievable by the covariance matrix of the maximum likelihood estimates when SNR is high.

Since the noise matrices $\mathbf{W}_A$ and $\mathbf{W}_B$ consist of i.i.d. $\mathcal{CN}(0,1)$ elements, the joint PDF of $\mathbf{Y}_A$ and $\mathbf{Y}'_B$ is

$$f(\mathbf{Y}_A, \mathbf{Y}'_B) = K_0\exp(-J) \quad (86)$$

where K_0 is a constant and J is given in (74). It follows that for any parameter θ, we have $\frac{\partial \ln f}{\partial \theta} = -\frac{\partial J}{\partial \theta}$. One can verify from (74) that $\frac{\partial J}{\partial \mathbf{H}} = -2\mathbf{W}_A\mathbf{X}_B^H - 2\mathbf{X}_{A,\alpha}^*\mathbf{W}_{B,\alpha}^T - 2\mathbf{X}_{A,\beta}^*\mathbf{W}_{B,\beta}^T$, $\frac{\partial J}{\partial \mathbf{U}_0} = 2\mathbf{H}^H\mathbf{W}_{A,\alpha} - 2\mathbf{W}_{B,\alpha}$, $\frac{\partial J}{\partial \mathbf{U}_1} = -2\mathbf{W}_{B,\beta}$ and $\frac{\partial J}{\partial \mathbf{U}_2} = 2\mathbf{H}^H\mathbf{W}_{A,\beta}$.

The above equations imply that the Fisher information matrix of the normalized unknowns $\mathbf{H}$, $\frac{1}{\sqrt{P}}\mathbf{U}_0$, $\frac{1}{\sqrt{P}}\mathbf{U}_1$ and $\frac{1}{\sqrt{P}}\mathbf{U}_2$ has

the following structure:

$$\mathbf{F}=\begin{bmatrix}\mathbf{F}_{\mathbf{h},\mathbf{h}} & \sqrt{P}\mathbf{F}_{\mathbf{h},\mathbf{u}_0} & \sqrt{P}\mathbf{F}_{\mathbf{h},\mathbf{u}_1} & \sqrt{P}\mathbf{F}_{\mathbf{h},\mathbf{u}_2}\\ \sqrt{P}\mathbf{F}^T_{\mathbf{h},\mathbf{u}_0} & P\mathbf{F}_{\mathbf{u}_0,\mathbf{u}_0} & 0 & 0\\ \sqrt{P}\mathbf{F}^T_{\mathbf{h},\mathbf{u}_1} & 0 & P\mathbf{F}_{\mathbf{u}_1,\mathbf{u}_1} & 0\\ \sqrt{P}\mathbf{F}^T_{\mathbf{h},\mathbf{u}_2} & 0 & 0 & P\mathbf{F}_{\mathbf{u}_2,\mathbf{u}_2}\end{bmatrix} \tag{87}$$

where all nonzero entries are proportional to P. For each pair of complex vectors $\mathbf{x}$ and $\mathbf{y}$, $\mathbf{F}_{\mathbf{x},\mathbf{y}}$ has the following form:

$$\begin{aligned}\mathbf{F}_{\mathbf{x},\mathbf{y}}&=\begin{bmatrix}\mathbf{F}_{\Re(\mathbf{x}),\Re(\mathbf{y})} & \mathbf{F}_{\Re(\mathbf{x}),\Im(\mathbf{y})}\\ \mathbf{F}_{\Im(\mathbf{x}),\Re(\mathbf{y})} & \mathbf{F}_{\Im(\mathbf{x}),\Im(\mathbf{y})}\end{bmatrix}\\ &=\begin{bmatrix}\mathbb{E}\left\{\frac{\partial J}{\partial\Re(\mathbf{x})}\frac{\partial J}{\partial\Re(\mathbf{y})^T}\right\} & \mathbb{E}\left\{\frac{\partial J}{\partial\Re(\mathbf{x})}\frac{\partial J}{\partial\Im(\mathbf{y})^T}\right\}\\ \mathbb{E}\left\{\frac{\partial J}{\partial\Im(\mathbf{x})}\frac{\partial J}{\partial\Re(\mathbf{y})^T}\right\} & \mathbb{E}\left\{\frac{\partial J}{\partial\Im(\mathbf{x})}\frac{\partial J}{\partial\Im(\mathbf{y})^T}\right\}\end{bmatrix}\end{aligned} \tag{88}$$

where the expectations are over the noise. Note that $\frac{\partial J}{\partial\Re(\mathbf{x})}=\frac{1}{2}(\frac{\partial J}{\partial\mathbf{x}}+(\frac{\partial J}{\partial\mathbf{x}})^*)$ and $\frac{\partial J}{\partial\Im(\mathbf{x})}=\frac{1}{2}(-j\frac{\partial J}{\partial\mathbf{x}}+j(\frac{\partial J}{\partial\mathbf{x}})^*)$. Also note that for $\mathbf{w}$ with the PDF $\mathcal{CN}(0,\mathbf{I})$, we have $\mathbb{E}\{\mathbf{w}\mathbf{w}^T\}=0$ and $\mathbb{E}\{\mathbf{w}\mathbf{w}^H\}=\mathbf{I}$. Further details of the nonzero entries in (87) are given next.

One can verify that $\mathbf{F}_{\Re(\mathbf{h}),\Re(\mathbf{h})}=\mathbf{F}_{\Im(\mathbf{h}),\Im(\mathbf{h})}=2\Re(\mathbf{X}^*_B\mathbf{X}^T_B\otimes\mathbf{I}_{n_A})+2\Re(\mathbf{I}_{n_B}\otimes\mathbf{X}^*_A\mathbf{X}^T_A)$, $\mathbf{F}_{\Re(\mathbf{h}),\Im(\mathbf{h})}=\mathbf{F}^T_{\Im(\mathbf{h}),\Re(\mathbf{h})}=-2\Im(\mathbf{X}^*_B\mathbf{X}^T_B\otimes\mathbf{I}_{n_A})-2\Im(\mathbf{I}_{n_B}\otimes\mathbf{X}^*_A\mathbf{X}^T_A)$, $\mathbf{F}_{\Re(\mathbf{u}_0),\Re(\mathbf{u}_0)}=\mathbf{F}_{\Im(\mathbf{u}_0),\Im(\mathbf{u}_0)}=2\Re(\mathbf{I}_{n_B}\otimes\mathbf{H}^T\mathbf{H}^*)+2\mathbf{I}_{n_B^2}$, $\mathbf{F}_{\Re(\mathbf{u}_0),\Im(\mathbf{u}_0)}=\mathbf{F}^T_{\Im(\mathbf{u}_0),\Re(\mathbf{u}_0)}=2\Im(\mathbf{I}_{n_B}\otimes\mathbf{H}^T\mathbf{H}^*)$, $\mathbf{F}_{\Re(\mathbf{u}_1),\Re(\mathbf{u}_1)}=\mathbf{F}_{\Im(\mathbf{u}_1),\Im(\mathbf{u}_1)}=2\mathbf{I}_{n_B(m_A-n_B)}$, $\mathbf{F}_{\Re(\mathbf{u}_1),\Im(\mathbf{u}_1)}=\mathbf{F}^T_{\Im(\mathbf{u}_1),\Re(\mathbf{u}_1)}=0$, $\mathbf{F}_{\Re(\mathbf{u}_2),\Re(\mathbf{u}_2)}=\mathbf{F}_{\Im(\mathbf{u}_2),\Im(\mathbf{u}_2)}=2\Re(\mathbf{I}_{m_B-n_B}\otimes\mathbf{H}^T\mathbf{H}^*)$ and $\mathbf{F}_{\Re(\mathbf{u}_2),\Im(\mathbf{u}_2)}=\mathbf{F}^T_{\Im(\mathbf{u}_2),\Re(\mathbf{u}_2)}=2\Im(\mathbf{I}_{m_B-n_B}\otimes\mathbf{H}^T\mathbf{H}^*)$.

To derive the cross-correlations between $\frac{\partial J}{\partial\mathbf{h}}$, $\frac{\partial J}{\partial\mathbf{u}_0}$, $\frac{\partial J}{\partial\mathbf{u}_1}$ and $\frac{\partial J}{\partial\mathbf{u}_2}$, it is helpful to use $\mathbf{A}=\mathbf{X}^*_B\otimes\mathbf{I}_{n_A}$, $\mathbf{B}=\mathbf{I}_{n_B}\otimes\mathbf{X}^*_A$, $\mathbf{C}=\mathbf{I}_{n_B}\otimes\mathbf{H}^H$ and $\mathbf{D}=\mathbf{I}_{m_B-n_B}\otimes\mathbf{H}^H$. Also use $\mathbf{A}_\alpha=\mathbf{X}^*_{B,\alpha}\otimes\mathbf{I}_{n_A}$, $\mathbf{A}_\beta=\mathbf{X}^*_{B,\beta}\otimes\mathbf{I}_{n_A}$, $\mathbf{B}_\alpha=\mathbf{I}_{n_B}\otimes\mathbf{X}^*_{A,\alpha}$ and $\mathbf{B}_\beta=\mathbf{I}_{n_B}\otimes\mathbf{X}^*_{A,\beta}$.

Then, one can verify that $\mathbf{F}_{\Re(\mathbf{h}),\Re(\mathbf{u}_0)}=-2\Re\{\mathbf{A}\mathbb{E}\{\mathbf{w}_A\mathbf{w}^H_{A,\alpha}\}\mathbf{C}^H\}+2\Re\{\mathbf{B}_\alpha\mathbb{E}\{\mathbf{w}_{B,\alpha,t}\mathbf{w}^H_{B,\alpha}\}\}$. Here $\mathbb{E}\{\mathbf{w}_A\mathbf{w}^H_{A,\alpha}\}$ equals the first n_An_B columns of $\mathbf{I}_{n_An_B}$, and hence $\mathbf{A}\mathbb{E}\{\mathbf{w}_A\mathbf{w}^H_{A,\alpha}\}=\mathbf{A}_\alpha$. Let $\mathbf{P}_{B,\alpha}$ and $\mathbf{P}_{B,\beta}$ be the permutations such that $\mathbf{w}_{B,\alpha,t}=\mathbf{P}_{B,\alpha}\mathbf{w}_{B,\alpha}$ and $\mathbf{w}_{B,\beta,t}=\mathbf{P}_{B,\beta}\mathbf{w}_{B,\beta}$. Then, $\mathbf{F}_{\Re(\mathbf{h}),\Re(\mathbf{u}_0)}=-2\Re\{\mathbf{X}^*_{B,\alpha}\otimes\mathbf{H}\}+2\Re\{(\mathbf{I}_{n_B}\otimes\mathbf{X}^*_{A,\alpha})\mathbf{P}_{B,\alpha}\}$. Similarly, one can verify that $\mathbf{F}_{\Re(\mathbf{h}),\Re(\mathbf{u}_0)}=\mathbf{F}_{\Im(\mathbf{h}),\Im(\mathbf{u}_0)}$, $\mathbf{F}_{\Re(\mathbf{h}),\Im(\mathbf{u}_0)}=-\mathbf{F}_{\Im(\mathbf{h}),\Re(\mathbf{u}_0)}$ and $\mathbf{F}_{\Re(\mathbf{h}),\Im(\mathbf{u}_0)}=2\Im\{\mathbf{X}^*_{B,\alpha}\otimes\mathbf{H}\}-2\Im\{(\mathbf{I}_{n_B}\otimes\mathbf{X}^*_{A,\alpha})\mathbf{P}_{B,\alpha}\}$. Furthermore, with $\mathbf{B}_\beta=\mathbf{I}_{n_B}\otimes\mathbf{X}^*_{A,\beta}$, we have $\mathbf{F}_{\Re(\mathbf{h}),\Re(\mathbf{u}_1)}=\mathbf{F}_{\Im(\mathbf{h}),\Im(\mathbf{u}_1)}=2\Re(\mathbf{B}_\beta)\mathbf{P}_{B,\beta}$ and $\mathbf{F}_{\Re(\mathbf{h}),\Im(\mathbf{u}_1)}=-\mathbf{F}_{\Im(\mathbf{h}),\Re(\mathbf{u}_1)}=-2\Im(\mathbf{B}_\beta)\mathbf{P}_{B,\beta}$. And with $\mathbf{A}_\beta=\mathbf{X}^*_{B,\beta}\otimes\mathbf{I}_{n_A}$ and $\mathbf{D}=\mathbf{I}_{m_B-n_B}\otimes\mathbf{H}^H$, we have $\mathbf{F}_{\Re(\mathbf{h}),\Re(\mathbf{u}_2)}=\mathbf{F}_{\Im(\mathbf{h}),\Im(\mathbf{u}_2)}=-2\Re(\mathbf{A}_\beta\mathbf{D}^H)$ and $\mathbf{F}_{\Re(\mathbf{h}),\Im(\mathbf{u}_2)}=-\mathbf{F}_{\Im(\mathbf{h}),\Re(\mathbf{u}_2)}=2\Im(\mathbf{A}_\beta\mathbf{D}^H)$.

The Cramer-Rao lower bound (CRLB) on the covariance matrix of the maximum likelihood estimate of the real-valued unknown vector $\boldsymbol{\theta}$, i.e., the column-wise stack of $\Re(\mathbf{h})$, $\Im(\mathbf{h})$, $\frac{1}{\sqrt{P}}\Re(\mathbf{u}_0)$, $\frac{1}{\sqrt{P}}\Im(\mathbf{u}_0)$, $\frac{1}{\sqrt{P}}\Re(\mathbf{u}_1)$, $\frac{1}{\sqrt{P}}\Im(\mathbf{u}_1)$, $\frac{1}{\sqrt{P}}\Re(\mathbf{u}_2)$ and $\frac{1}{\sqrt{P}}\Im(\mathbf{u}_2)$) is given by the inverse matrix $\mathbf{F}^{-1}$. If any parameters in $\boldsymbol{\theta}$ become known, the corresponding Fisher information matrix is still given by $\mathbf{F}$ but with the corresponding columns and rows removed.

If $\mathbf{H}$ is given, the CRLBs for $\frac{1}{\sqrt{P}}\mathbf{u}_0$, $\frac{1}{\sqrt{P}}\mathbf{u}_1$ and $\frac{1}{\sqrt{P}}\mathbf{u}_2$ are respectively $\frac{1}{P}\mathbf{F}^{-1}_{\mathbf{u}_0,\mathbf{u}_0}$, $\frac{1}{P}\mathbf{F}^{-1}_{\mathbf{u}_1,\mathbf{u}_1}$ and $\frac{1}{P}\mathbf{F}^{-1}_{\mathbf{u}_2,\mathbf{u}_2}$. The corresponding lower bounds on the (per-complex-element) estimation variances of $\frac{1}{\sqrt{P}}\mathbf{u}_0$, $\frac{1}{\sqrt{P}}\mathbf{u}_1$ and $\frac{1}{\sqrt{P}}\mathbf{u}_2$ are respectively $\frac{1}{Pn_B^2}Tr(\mathbf{F}^{-1}_{\mathbf{u}_0,\mathbf{u}_0})$, $\frac{1}{Pn_B(m_A-n_B)}Tr(\mathbf{F}^{-1}_{\mathbf{u}_1,\mathbf{u}_1})$ and $\frac{1}{Pn_B(m_B-n_B)}Tr(\mathbf{F}^{-1}_{\mathbf{u}_2,\mathbf{u}_2})$. Note that these bounds are independent of $\mathbf{X}_A$ and $\mathbf{X}_B$. Furthermore, $\frac{1}{P}\mathbf{F}^{-1}_{\mathbf{u}_1,\mathbf{u}_1}=\frac{1}{2P}\mathbf{I}_{2n_B(m_A-n_B)}$ which is uniform and invariant to any unknowns. This property for $\mathbf{u}_1$ (whose dimension increases with m_A) should be quite useful in practice.

IX. Secret Key Capacity After Pre-Processing

In this section, we provide the proof of Theorem 2 and Corollaries shown in Section VII. For the proposed pre-processing method, additional data are communicated publicly. The data sets available at Alice, Bob and Eve are now changed from $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$ to $\mathcal{X}'$, $\mathcal{Y}'$ and $\mathcal{Z}'$, respectively, where $\mathcal{X}'=\{\mathcal{X},\mathbf{X}'_B,\mathbf{Y}'_B\}$, $\mathcal{Y}'=\{\mathcal{Y},\mathbf{U}\}$ and $\mathcal{Z}'=\{\mathcal{Z},\mathbf{X}'_B,\mathbf{Y}'_B\}$. Also remember the assumption $n_A\geq n_B$.

Now the secret key capacity of the new model is denoted by C'_S which satisfies $\max(C'_A,C'_B)\leq C'_S\leq C'_Z$ where $C'_A=h(\mathcal{X}'|\mathcal{Z}')-h(\mathcal{X}'|\mathcal{Y}')$, $C'_B=h(\mathcal{Y}'|\mathcal{Z}')-h(\mathcal{Y}'|\mathcal{X}')$ and $C'_Z=h(\mathcal{Y}'|\mathcal{Z}')-h(\mathcal{Y}'|\mathcal{X}',\mathcal{Z}')$. We will show next in Section IX-A that $DoF(h(\mathcal{Y}'|\mathcal{X}'))=0$ and hence $DoF(h(\mathcal{Y}'|\mathcal{X}',\mathcal{Z}'))=0$, and therefore

$$DoF(C'_S)=DoF(C'_Z)=DoF(C'_B)=DoF(h(\mathcal{Y}'|\mathcal{Z}')), \tag{89}$$

which will further be shown to be (103) in Section IX-B. We will also show in Section IX-C that

$$DoF(C'_S)=DoF(C_S) \tag{90}$$

where the right side is given by (53) with $n_A\geq n_B$ and $|\rho|=1$, which leads to Theorem 2.

In this section, we will also highlight key modifications needed to prove Corollaries 1 and 2.

A. Proof of $DoF(h(\mathcal{Y}'|\mathcal{X}'))=0$

We know

$$\begin{aligned}h(\mathcal{Y}'|\mathcal{X}')&=h(\mathbf{X}_B,\mathbf{Y}_B,\mathbf{U}|\mathcal{X}')\\ &=h(\mathbf{X}_B|\mathcal{X}')+h(\mathbf{Y}_B|\mathbf{X}_B,\mathcal{X}')\\ &\quad+h(\mathbf{U}|\mathbf{X}_B,\mathbf{Y}_B,\mathcal{X}').\end{aligned} \tag{91}$$

It is shown next that each of the three terms in (91) has zero DoF.

Note that for Corollaries 1 and 2, there are public constraints on $\mathbf{U}$. Those constraints do not change the property $DoF(h(\mathcal{Y}'|\mathcal{X}'))=0$. In fact, those constraints make $\mathcal{Y}'$ somewhat "more determined" by $\mathcal{X}'$.

1) Proof of $DoF(h(\mathbf{X}_B|\mathcal{X}'))=0$: Here

$$\begin{aligned}&h(\mathbf{X}_B|\mathcal{X}')=h(\mathbf{X}_B|\mathbf{X}_A,\mathbf{Y}_A,\mathbf{X}'_B,\mathbf{Y}'_B)\\ &=h(\mathbf{Y}_A,\mathbf{X}'_B,\mathbf{Y}'_B|\mathbf{X}_A,\mathbf{X}_B)+h(\mathbf{X}_B|\mathbf{X}_A)\\ &\quad-h(\mathbf{Y}_A,\mathbf{X}'_B,\mathbf{Y}'_B|\mathbf{X}_A)\\ &=h(\mathbf{Y}_A|\mathbf{X}_B)+h(\mathbf{X}'_B|\mathbf{Y}_A,\mathbf{X}_B)+h(\mathbf{Y}'_B|\mathbf{X}_A,\mathbf{Y}_A,\mathbf{X}'_B,\mathbf{X}_B)\\ &\quad+h(\mathbf{X}_B)-h(\mathbf{X}'_B)-h(\mathbf{Y}_A|\mathbf{X}'_B)-h(\mathbf{Y}'_B|\mathbf{X}_A,\mathbf{X}'_B,\mathbf{Y}_A)\end{aligned} \tag{92}$$

where we have dropped the condition on $\mathbf{X}_A$ in several terms when it is independent of all other matrices of interest. It is clear that $DoF(h(\mathbf{X}_B)) = DoF(h(\mathbf{X}'_B)) = n_B m_B$, $DoF(h(\mathbf{Y}_A|\mathbf{X}_B)) = n_A n_B$ and $DoF(h(\mathbf{X}'_B|\mathbf{Y}_A, \mathbf{X}_B)) = DoF(h(\mathbf{X}'_B|\mathbf{X}_B)) = n_B m_B$. Also $DoF(h(\mathbf{Y}_A|\mathbf{X}'_B)) = DoF(h(\mathbf{Y}_A)) = n_B m_B + (n_A - n_B)n_B$, which follows from a similar analysis as for (27). The other two terms $h(\mathbf{Y}'_B|\mathbf{X}_A, \mathbf{Y}_A, \mathbf{X}'_B, \mathbf{X}_B)$ and $h(\mathbf{Y}'_B|\mathbf{X}_A, \mathbf{X}'_B, \mathbf{Y}_A)$ in (92) are discussed below.

We know $DoF(h(\mathbf{Y}'_B|\mathbf{X}_A, \mathbf{Y}_A, \mathbf{X}'_B, \mathbf{X}_B)) = DoF(h(\mathbf{Y}'_B|\mathbf{X}_A, \mathbf{U}_0, \mathbf{H}_{A,B}))$ where we have applied that $\{\mathbf{Y}_A, \mathbf{X}_B\}$ determines $\mathbf{H}_{A,B}$ at a high power P, $\{\mathbf{X}'_B, \mathbf{X}_B\}$ determines $[\mathbf{U}_0, \mathbf{U}_2]$, and, given $\{\mathbf{X}_A, \mathbf{U}_0, \mathbf{H}_{A,B}\}$, $\mathbf{Y}'_B$ is independent of $\{\mathbf{Y}_A, \mathbf{X}'_B, \mathbf{X}_B\}$. Furthermore

$$\begin{aligned} h(\mathbf{Y}'_B|\mathbf{X}_A, \mathbf{U}_0, \mathbf{H}_{A,B}) &= h(\mathbf{Y}'_{B,\alpha}|\mathbf{X}_A, \mathbf{U}_0, \mathbf{H}_{A,B}) \\ &\quad + h(\mathbf{Y}'_{B,\beta}|\mathbf{X}_A, \mathbf{Y}'_{B,\alpha}, \mathbf{U}_0, \mathbf{H}_{A,B}) \\ &= h(\mathbf{Y}_{B,\alpha}|\mathbf{X}_A, \mathbf{H}_{A,B}) + h(\mathbf{Y}'_{B,\beta}|\mathbf{X}_A, \mathbf{H}_{A,B}). \end{aligned} \tag{93}$$

We also know that $DoF(h(\mathbf{Y}_{B,\alpha}|\mathbf{X}_A, \mathbf{H}_{A,B})) = 0$ and $DoF(h(\mathbf{Y}'_{B,\beta}|\mathbf{X}_A, \mathbf{H}_{A,B}) = DoF(h(\mathbf{U}_1)) = n_B(m_A - n_B)$. Therefore,

$$DoF(h(\mathbf{Y}'_B|\mathbf{X}_A, \mathbf{Y}_A, \mathbf{X}'_B, \mathbf{X}_B)) = n_B(m_A - n_B). \tag{94}$$

Now we consider

$$\begin{aligned} h(\mathbf{Y}'_B|\mathbf{X}_A, \mathbf{X}'_B, \mathbf{Y}_A) &= h(\mathbf{Y}'_{B,\alpha}|\mathbf{X}_A, \mathbf{X}'_B, \mathbf{Y}_A) \\ &\quad + h(\mathbf{Y}'_{B,\beta}|\mathbf{Y}'_{B,\alpha}, \mathbf{X}_A, \mathbf{X}'_B, \mathbf{Y}_A). \end{aligned} \tag{95}$$

where we recall $\mathbf{Y}'_{B,\alpha} = \mathbf{H}_{B,A}\mathbf{X}_{A,\alpha} + \mathbf{U}_0 + \mathbf{W}_{B,\alpha}$, $\mathbf{Y}'_{B,\beta} = \mathbf{H}_{B,A}\mathbf{X}_{A,\beta} + \mathbf{U}_1 + \mathbf{W}_{B,\beta}$, $\mathbf{X}'_B = \mathbf{X}_B + [\mathbf{U}_0, \mathbf{U}_2]$ and $\mathbf{Y}_A = \mathbf{H}_{A,B}\mathbf{X}_B + \mathbf{W}_A$. Since $\mathbf{U}_1$ is independent of $\{\mathbf{Y}'_{B,\alpha}, \mathbf{X}_A, \mathbf{X}'_B, \mathbf{Y}_A\}$, and $\{\mathbf{X}_{B,\alpha}, \mathbf{Y}_{A,\alpha}\}$ determines $\mathbf{H}_{A,B}$ at high power, we have $DoF(h(\mathbf{Y}'_{B,\beta}|\mathbf{Y}'_{B,\alpha}, \mathbf{X}_A, \mathbf{X}'_B, \mathbf{Y}_A)) \geq DoF(h(\mathbf{Y}'_{B,\beta}|\mathbf{X}_{B,\alpha}, \mathbf{Y}'_{B,\alpha}, \mathbf{X}_A, \mathbf{X}'_B, \mathbf{Y}_A)) = DoF(h(\mathbf{U}_1 + \mathbf{W}_{B,\beta})) = n_B(m_A - n_B)$. Since $\mathbf{Y}'_{B,\beta}$ has the dimension $n_B \times (m_A - n_B)$, $DoF(h(\mathbf{Y}'_{B,\beta}|*) \leq n_B(m_A - n_B)$. Therefore,

$$DoF(h(\mathbf{Y}'_{B,\beta}|\mathbf{Y}'_{B,\alpha}, \mathbf{X}_A, \mathbf{X}'_B, \mathbf{Y}_A)) = n_B(m_A - n_B). \tag{96}$$

Since $\mathbf{Y}'_{B,\alpha}$ has the dimension $n_B \times n_B$, $DoF(h(\mathbf{Y}'_{B,\alpha}|*)) \leq n_B^2$. We show next that

$$DoF(h(\mathbf{Y}'_{B,\alpha}|\mathbf{X}_A, \mathbf{X}'_B, \mathbf{Y}_A)) = n_B^2. \tag{97}$$

To prove (97), we consider $h(\mathbf{Y}'_{B,\alpha}|\mathbf{X}_A, \mathbf{X}'_B, \mathbf{Y}_A) \geq h(\mathbf{Y}'_{B,\alpha}|\mathbf{X}_{A,\alpha}, \mathbf{X}'_{B,\alpha}, \mathbf{Y}_{A,\alpha})$. It is now sufficient to prove $DoF(h(\mathbf{Y}'_{B,\alpha}|\mathbf{X}_{A,\alpha}, \mathbf{X}'_{B,\alpha}, \mathbf{Y}_{A,\alpha})) = n_B^2$. There is a little complexity due to the product $\mathbf{H}_{A,B}\mathbf{X}_B$ of two random matrices in $\mathbf{Y}_A$. But we can get around this problem by applying the chain rule of differential entropy to the total n_B^2 (complex) elements in $\mathbf{Y}'_{B,\alpha}$ and show that each of the n_B^2 terms has its DoF equal to one. It suffices to show that at a high power none of the elements in $\mathbf{Y}'_{B,\alpha}$ can be consistently estimated from all other elements in $\mathbf{Y}'_{B,\alpha}$ along with the knowledge of $\{\mathbf{X}_{A,\alpha}, \mathbf{X}'_{B,\alpha}, \mathbf{Y}_{A,\alpha}\}$. Indeed, any $n_B^2 - 1$ elements in $\mathbf{Y}'_{B,\alpha}$ along with the $n_B^2 + 2n_A n_B$ elements in $\{\mathbf{X}_{A,\alpha}, \mathbf{X}'_{B,\alpha}, \mathbf{Y}_{A,\alpha}\}$ constitute $2n_B^2 + 2n_A n_B - 1$ known equations. The corresponding unknowns are the $n_A n_B$ elements in $\mathbf{X}_{A,\alpha}$, the n_B^2 elements in $\mathbf{X}_{B,\alpha}$, the n_B^2 elements in $\mathbf{U}_0$ and the $n_A n_B$ elements in $\mathbf{H}_{A,B}$. We see that there is an extra degree of freedom in the unknowns. Hence, no element of $\mathbf{Y}'_{B,\alpha}$ can be consistently estimated from all other elements in $\mathbf{Y}'_{B,\alpha}$ along with $\{\mathbf{X}_{A,\alpha}, \mathbf{X}'_{B,\alpha}, \mathbf{Y}_{A,\alpha}\}$. Therefore, (97) holds.

Using (97) and (96) in (95) yields

$$DoF(h(\mathbf{Y}'_B|\mathbf{X}_A, \mathbf{X}'_B, \mathbf{Y}_A)) = n_B m_A. \tag{98}$$

Then applying (98), (94) and other results below (92) into (92), we have

$$DoF(h(\mathbf{X}_B|\mathcal{X}')) = 0. \tag{99}$$

Since $\mathcal{X}'$ includes $\mathbf{X}'_B = \mathbf{X}_B + [\mathbf{U}_0^*, \mathbf{U}_2]$, (99) suggests that, with $\mathcal{X}'$, Alice's ambiguity about $\{\mathbf{U}_0, \mathbf{U}_2\}$ does not increase as power increases. This coincides with the fact that Alice can obtain a consistent estimate of $\{\mathbf{U}_0, \mathbf{U}_2\}$ and hence $\mathbf{U}_1$ as power increases.

2) Proof of $DoF(h(\mathbf{Y}_B|\mathbf{X}_B, \mathcal{X}')) = 0$: Here

$$\begin{aligned} h(\mathbf{Y}_B|\mathbf{X}_B, \mathcal{X}') &= h(\mathbf{Y}_B|\mathbf{X}_B, \mathbf{X}_A, \mathbf{Y}_A, \mathbf{X}'_B, \mathbf{Y}'_B) \\ &\approx h(\mathbf{Y}_B|\mathbf{X}_A, \mathbf{H}_{A,B}) \end{aligned} \tag{100}$$

and therefore $DoF(h(\mathbf{Y}_B|\mathbf{X}_B, \mathcal{X}')) = 0$.

3) Proof of $DoF(h(\mathbf{U}|\mathbf{X}_B, \mathbf{Y}_B, \mathcal{X}')) = 0$: Here

$$\begin{aligned} h(\mathbf{U}|\mathbf{X}_B, \mathbf{Y}_B, \mathcal{X}') &= h(\mathbf{U}|\mathbf{X}_B, \mathbf{Y}_B, \mathbf{X}_A, \mathbf{Y}_A, \mathbf{X}'_B, \mathbf{Y}'_B) \\ &= h(\mathbf{U}|\mathbf{U}_0, \mathbf{U}_1, \mathbf{U}_2) \end{aligned} \tag{101}$$

and hence $DoF(h(\mathbf{U}|\mathbf{X}_B, \mathbf{Y}_B, \mathcal{X}')) = 0$.

B. Analysis of $h(\mathcal{Y}'|\mathcal{Z}')$

Since $\{\mathbf{X}'_B, \mathbf{Y}'_B\}$ is part of each of $\mathcal{Y}'$ and $\mathcal{Z}'$, we have

$$\begin{aligned} h(\mathcal{Y}'|\mathcal{Z}') &= h(\mathbf{X}_B, \mathbf{X}'_B, \mathbf{Y}_B, \mathbf{Y}'_B|\mathcal{Z}') = h(\mathbf{X}_B, \mathbf{Y}_B|\mathcal{Z}') \\ &= h(\mathbf{X}_B|\mathcal{Z}') + h(\mathbf{Y}_B|\mathbf{X}_B, \mathcal{Z}'). \end{aligned} \tag{102}$$

We show next in Sections IX-B1 and IX-B2 that

$$\begin{aligned} &DoF(h(\mathcal{Y}'|\mathcal{Z}')) \\ &= n_E n_B + n_B m_B - \min(n_B, n_E)m_B - (n_E - n_B)^+ n_B \\ &\quad + \min(n_B + n_E, n_A)m_A + (n_B + n_E - n_A)^+ n_A - n_B^2 \\ &\quad - \min(n_A, n_E)m_A - (n_E - n_A)^+ n_A - p, \end{aligned} \tag{103}$$

which can be simplified to

$$\begin{aligned} &DoF(h(\mathcal{Y}'|\mathcal{Z}')) \\ &= (n_B - n_E)^+(m_B - n_B) + \min(n_B, (n_A - n_E)^+)m_A \\ &\quad + \min(n_B, (n_B + n_E - n_A)^+)n_A - p. \end{aligned} \tag{104}$$

Here $p = 0$ for Theorem 2 where there is no additional constraint on $\mathbf{U}$; $p = 1$ for Corollary 1 where there is a complex scalar constraint on $\mathbf{U}_0$; and $p = p_0 + p_1 = n_A n_B$ with $p_0 = n_B^2$ and $p_1 = n_B(n_A - n_B)$ for Corollary 2 where $\mathbf{U}_0$ and the first $n_A - n_B$ columns of $\mathbf{U}_1$ are public, or equivalently, $\mathbf{X}_{B,\alpha}$ and the first n_A columns of $\mathbf{Y}_B$ are public.

1) Analysis of $h(\mathbf{X}_B|\mathcal{Z}')$: We know

$$\begin{aligned} h(\mathbf{X}_B|\mathcal{Z}') &= h(\mathbf{X}_B|\mathcal{Z}, \mathbf{X}'_B, \mathbf{Y}'_B) \\ &= h(\mathbf{X}'_B|\mathcal{Z}, \mathbf{X}_B, \mathbf{Y}'_B) + h(\mathbf{X}_B|\mathcal{Z}, \mathbf{Y}'_B) \\ &\quad - h(\mathbf{X}'_B|\mathcal{Z}, \mathbf{Y}'_B). \end{aligned} \tag{105}$$

Here $h(\mathbf{X}'_B|\mathcal{Z},\mathbf{X}_B,\mathbf{Y}'_B)=h(\mathbf{U}_0,\mathbf{U}_2|\mathbf{Y}_{E,A},\mathbf{Y}'_B)$ after dropping the conditioning components $\{\mathbf{X}_B,\mathbf{Y}_{E,B}\}$ that are independent of $\{\mathbf{U}_0,\mathbf{U}_2,\mathbf{Y}_{E,A},\mathbf{Y}'_B\}$. For Corollaries 1 and 2, this equality also holds but subject to the scalar constraint on $\mathbf{U}_0$ for Corollary 1 or $\mathbf{U}_0$ being public for Corollary 2.

So, the first term in (105) is

$$\begin{aligned}&h(\mathbf{X}'_B|\mathcal{Z},\mathbf{X}_B,\mathbf{Y}'_B)=h(\mathbf{U}_0,\mathbf{U}_2|\mathbf{Y}_{E,A},\mathbf{Y}'_B)\\&=h(\mathbf{U}_0|\mathbf{Y}_{E,A},\mathbf{Y}'_B)+h(\mathbf{U}_2)\\&=h(\mathbf{Y}_{E,A},\mathbf{Y}'_B|\mathbf{U}_0)+h(\mathbf{U}_0)-h(\mathbf{Y}_{E,A},\mathbf{Y}'_B)\\&\quad+h(\mathbf{U}_2).\end{aligned}\tag{106}$$

We now show that $DoF(h(\mathbf{Y}_{E,A},\mathbf{Y}'_B|\mathbf{U}_0))=DoF(h(\mathbf{Y}_{E,A},\mathbf{Y}'_B))$. First, we can write $h(\mathbf{Y}_{E,A},\mathbf{Y}'_B|\mathbf{U}_0)=h(\mathbf{Y}_{E,A})+h(\mathbf{Y}'_B|\mathbf{Y}_{E,A},\mathbf{U}_0)=h(\mathbf{Y}_{E,A})+h(\mathbf{Y}_{B,\alpha}|\mathbf{Y}_{E,A})+h(\mathbf{Y}_{B,\beta}+\mathbf{U}_1|\mathbf{Y}_{E,A})$ and $h(\mathbf{Y}_{E,A},\mathbf{Y}'_B)=h(\mathbf{Y}_{E,A})+h(\mathbf{Y}'_B|\mathbf{Y}_{E,A})$. We know that $n_B^2=DoF(h(\mathbf{Y}_{B,\alpha}|\mathbf{X}_{A,\alpha},\mathbf{Y}_{E,A}))\le DoF(h(\mathbf{Y}_{B,\alpha}|\mathbf{Y}_{E,A}))\le DoF(h(\mathbf{Y}_{B,\alpha}))\le n_B^2$, $DoF(h(\mathbf{Y}_{B,\beta}+\mathbf{U}_1|\mathbf{Y}_{E,A}))=DoF(h(\mathbf{U}_1))=n_B(m_A-n_B)$, $DoF(h(\mathbf{Y}'_B|\mathbf{Y}_{E,A}))=DoF(h(\mathbf{U}_0,\mathbf{U}_1))=n_Bm_A$. Hence, $DoF(h(\mathbf{Y}_{E,A},\mathbf{Y}'_B|\mathbf{U}_0))=DoF(h(\mathbf{Y}_{E,A},\mathbf{Y}'_B))$. One can verify that this equality also holds for Corollaries 1 and 2.

Then, (106) implies

$$\begin{aligned}DoF(h(\mathbf{X}'_B|\mathcal{Z},\mathbf{X}_B,\mathbf{Y}'_B))&=DoF(h(\mathbf{U}_0))+DoF(h(\mathbf{U}_2))\\&=n_Bm_B-p'.\end{aligned}\tag{107}$$

Here $p'=0$ for Theorem 2, $p'=1$ for Corollary 1, and $p'=p_0$ for Corollary 2.

The second term in (105) is $h(\mathbf{X}_B|\mathcal{Z},\mathbf{Y}'_B)=h(\mathbf{X}_B|\mathbf{Y}_{E,A},\mathbf{Y}_{E,B},\mathbf{Y}'_B)=h(\mathbf{X}_B|\mathbf{Y}_{E,B})=h(\mathbf{Y}_{E,B}|\mathbf{X}_B)+h(\mathbf{X}_B)-h(\mathbf{Y}_{E,B})$. Like (17), $DoF(h(\mathbf{Y}_{E,B}|\mathbf{X}_B))=n_En_B$. Like (27), $DoF(h(\mathbf{Y}_{E,B}))=\min(n_B,n_E)m_B+(n_E-n_B)^+n_B$. Also note that $DoF(h(\mathbf{X}_B))=n_Bm_B-p'$. Hence,

$$\begin{aligned}&DoF(h(\mathbf{X}_B|\mathcal{Z},\mathbf{Y}'_B))=DoF(h(\mathbf{X}_B|\mathbf{Y}_{E,B}))\\&=n_En_B+n_Bm_B-\min(n_B,n_E)m_B-(n_E-n_B)^+n_B\\&\quad-p'.\end{aligned}\tag{108}$$

The third term in (105) satisfies $h(\mathbf{X}'_B)\ge h(\mathbf{X}'_B|\mathcal{Z},\mathbf{Y}'_B)\ge h(\mathbf{X}'_B|\mathcal{Z},\mathbf{X}_B,\mathbf{Y}'_B)=h(\mathbf{U}_0,\mathbf{U}_2)$ where both the lower and upper bounds have the same DoF n_Bm_B-p', and hence

$$DoF(h(\mathbf{X}'_B|\mathcal{Z},\mathbf{Y}'_B))=n_Bm_B-p'.\tag{109}$$

Therefore, using (109), (108) and (107) in (105) results in

$$\begin{aligned}&DoF(h(\mathbf{X}_B|\mathcal{Z}'))=DoF(h(\mathbf{X}_B|\mathbf{Y}_{E,B}))\\&=n_En_B+n_Bm_B-\min(n_B,n_E)m_B-(n_E-n_B)^+n_B\\&\quad-p'.\end{aligned}\tag{110}$$

2) Analysis of $h(\mathbf{Y}_B|\mathbf{X}_B,\mathcal{Z}')$: We know

$$\begin{aligned}&h(\mathbf{Y}_B|\mathbf{X}_B,\mathcal{Z}')=h(\mathbf{Y}_B|\mathbf{X}_B,\mathbf{Y}_{E,A},\mathbf{Y}_{E,B},\mathbf{X}'_B,\mathbf{Y}'_B)\\&=h(\mathbf{Y}_B|\mathbf{U}_0,\mathbf{U}_2,\mathbf{Y}_{E,A},\mathbf{Y}'_B)\\&=h(\mathbf{Y}_B|\mathbf{U}_0,\mathbf{U}_2)+h(\mathbf{Y}_{E,A},\mathbf{Y}'_B|\mathbf{U}_0,\mathbf{U}_2,\mathbf{Y}_B)\\&\quad-h(\mathbf{Y}_{E,A},\mathbf{Y}'_B|\mathbf{U}_0,\mathbf{U}_2).\end{aligned}\tag{111}$$

Here, without the constraints in Corollaries 1 and 2, $DoF(h(\mathbf{Y}_B|\mathbf{U}_0,\mathbf{U}_2))=DoF(h(\mathbf{Y}_B))=n_Bm_A$ due to (27) with $n_A\ge n_B$. But with the possible constraints in Corollaries 1 and 2, we have

$$DoF(h(\mathbf{Y}_B|\mathbf{U}_0,\mathbf{U}_2))=n_Bm_A-p.\tag{112}$$

The second term in (111) is

$$\begin{aligned}&h(\mathbf{Y}_{E,A},\mathbf{Y}'_B|\mathbf{U}_0,\mathbf{U}_2,\mathbf{Y}_B)=h(\mathbf{Y}_{E,A},\mathbf{U}_0,\mathbf{U}_1|\mathbf{U}_0,\mathbf{U}_2,\mathbf{Y}_B)\\&=h(\mathbf{Y}_{E,A},\mathbf{U}_1|\mathbf{Y}_B)=h(\mathbf{U}_1)+h(\mathbf{Y}_{E,A}|\mathbf{Y}_B)\\&=h(\mathbf{U}_1)+h(\mathbf{Y}_{E,A},\mathbf{Y}_B)-h(\mathbf{Y}_B).\end{aligned}\tag{113}$$

The impact of the public constraints in Corollaries 1 and 2 on the DoF of $h(\mathbf{Y}_{E,A},\mathbf{Y}_B)$ and $h(\mathbf{Y}_B)$ in $h(\mathbf{Y}_{E,A},\mathbf{Y}_B)-h(\mathbf{Y}_B)$ cancels each other. But $DoF(h(\mathbf{U}_1))=n_B(m_A-n_B)-p''$ where $p''=0$ for Theorem 2 and Corollary 1 and $p''=n_B(n_A-n_B)$ for Corollary 2. Also using (27) and (46), it follows that

$$\begin{aligned}&DoF(h(\mathbf{Y}_{E,A},\mathbf{Y}'_B|\mathbf{U}_0,\mathbf{U}_2,\mathbf{Y}_B))\\&=\min(n_B+n_E,n_A)m_A+(n_B+n_E-n_A)^+n_A-n_B^2\\&\quad-p''.\end{aligned}\tag{114}$$

The third term in (111) is

$$\begin{aligned}&h(\mathbf{Y}_{E,A},\mathbf{Y}'_B|\mathbf{U}_0,\mathbf{U}_2)=h(\mathbf{Y}_{E,A})+h(\mathbf{Y}'_B|\mathbf{Y}_{E,A},\mathbf{U}_0)\\&=h(\mathbf{Y}_{E,A})+h(\mathbf{Y}'_{B,\alpha}|\mathbf{Y}_{E,A},\mathbf{U}_0)\\&\quad+h(\mathbf{Y}'_{B,\beta}|\mathbf{Y}'_{B,\alpha},\mathbf{Y}_{E,A},\mathbf{U}_0)\\&=h(\mathbf{Y}_{E,A})+h(\mathbf{Y}_{B,\alpha}|\mathbf{Y}_{E,A})+h(\mathbf{Y}'_{B,\beta}|\mathbf{Y}'_{B,\alpha},\mathbf{Y}_{E,A}).\end{aligned}\tag{115}$$

Here $DoF(h(\mathbf{Y}_{E,A}))$ is given by (35). Without the constraints in Corollaries 1 and 2, we know $n_B^2\ge DoF(h(\mathbf{Y}_{B,\alpha}|\mathbf{Y}_{E,A}))\ge DoF(h(\mathbf{Y}_{B,\alpha}|\mathbf{X}_{A,\alpha},\mathbf{Y}_{E,A}))=n_B^2$ and $n_B(m_A-n_B)\ge DoF(h(\mathbf{Y}'_{B,\beta}|\mathbf{Y}'_{B,\alpha},\mathbf{Y}_{E,A}))\ge DoF(h(\mathbf{Y}'_{B,\beta}|\mathbf{H}_{B,A},\mathbf{X}_A,\mathbf{Y}'_{B,\alpha},\mathbf{Y}_{E,A}))=DoF(h(\mathbf{U}_1))=n_B(m_A-n_B)$. But with the possible constraints in Corollaries 1 and 2, we have $DoF(h(\mathbf{Y}_{B,\alpha}|\mathbf{Y}_{E,A}))=n_B^2-p'$ and $DoF(h(\mathbf{Y}'_{B,\beta}|\mathbf{Y}'_{B,\alpha},\mathbf{Y}_{E,A}))=n_B(m_A-n_B)-p''$. Therefore,

$$\begin{aligned}&DoF(h(\mathbf{Y}_{E,A},\mathbf{Y}'_B|\mathbf{U}_0,\mathbf{U}_2))\\&=\min(n_A,n_E)m_A+(n_E-n_A)^+n_A+n_Bm_A-p\end{aligned}\tag{116}$$

where $p=p'+p''$.

It follows from (111) with (112), (114) and (116) that

$$\begin{aligned}&DoF(h(\mathbf{Y}_B|\mathbf{X}_B,\mathcal{Z}'))\\&=\min(n_B+n_E,n_A)m_A+(n_B+n_E-n_A)^+n_A-n_B^2\\&\quad-\min(n_A,n_E)m_A-(n_E-n_A)^+n_A-p''.\end{aligned}\tag{117}$$

Finally, by adding (110) and (117), we have (103).

C. Gap Between $DoF(C_S)$ and $DoF(C'_S)$

To compare $DoF(C_S)$ shown in (53) and $DoF(C'_S)$ shown in (103), one can verify that either if $|\rho|=1$ and there is no additional constraint on $\mathbf{U}$ as in Theorem 2, or if $|\rho|<1$ and there are additional constraints on $\mathbf{U}$ as in Corollary 2, then $DoF(C_S)-DoF(C'_S)=(n_A+n_E-n_B)^+n_B-n_An_B-n_En_B+n_B^2=0$ for all $n_E\ge 0$ subject to $n_A\ge n_B\ge 1$. But for Corollary 1, $DoF(C_S)-DoF(C'_S)=1$.

X. Using Public Pilots and Random Symbols

In this section we consider the situation where the first n_A columns of $\mathbf{X}_A$ and the first n_B columns of $\mathbf{X}_B$ are nonsingular and publicly known. Equivalently, we have $\mathbf{X}_A = [\mathbf{X}_{A,a}, \mathbf{X}_{A,b}]$ and $\mathbf{X}_B = [\mathbf{X}_{B,a}, \mathbf{X}_{B,b}]$ where $\mathbf{X}_{A,a}$ and $\mathbf{X}_{B,a}$ are nonsingular constant matrices but $\mathbf{X}_{A,b}$ and $\mathbf{X}_{B,b}$ are random matrices consisting of i.i.d. $\mathcal{CN}(0, P)$ entries. We still assume that the power of each entry of $\mathbf{X}_A$ and $\mathbf{X}_B$ is P (unless mentioned otherwise later regarding (146)). We will show the following theorem:

Theorem 3: By embedding nonsingular public pilots in the transmissions from Alice and Bob during GCP, there is no loss of DoF of secret key capacity from that shown in (7) of Theorem 1.

Proof: The proof consists of the following Sections X-A1, X-A2, X-A3 and X-A4.

1) Analysis of $h(\mathcal{X}|\mathcal{Y})$: Notice that (13) and (14) still hold. But unlike (15), we now have

$$DoF(h(\mathbf{X}_A)) = n_A(m_A - n_A). \tag{118}$$

It also follows from (16) where the expectation should be now treated as over the random parts of $\mathbf{X}_A$ that

$$DoF(h(\mathbf{Y}_B|\mathbf{X}_A)) = n_A n_B. \tag{119}$$

But unlike (27), $DoF(h(\mathbf{Y}_B))$ is shown next. Let $\mathbf{Y}_B = [\mathbf{Y}_{B,a}, \mathbf{Y}_{B,b}]$ where $\mathbf{Y}_{B,a}$ is the first n_A columns of $\mathbf{Y}_B$, and $\mathbf{Y}_{B,b}$ is the last $m_A - n_A$ columns of $\mathbf{Y}_B$. Correspondingly, we have $\mathbf{Y}_{B,a} = \mathbf{H}_{B,A}\mathbf{X}_{A,a} + \mathbf{W}_{B,a}$ and $\mathbf{Y}_{B,b} = \mathbf{H}_{B,A}\mathbf{X}_{A,b} + \mathbf{W}_{B,b}$. It follows that, noticing $rank(\mathbf{H}_{B,A}) = \min(n_A, n_B)$,

$$\begin{aligned} DoF(h(\mathbf{Y}_B)) &= DoF(h(\mathbf{Y}_{B,a})) + DoF(h(\mathbf{Y}_{B,b}|\mathbf{Y}_{B,a})) \\ &= n_A n_B + \min(n_A, n_B)(m_A - n_A) \end{aligned} \tag{120}$$

which differs from (27). Therefore, it follows from (14), (118), (119) and (120) that

$$DoF(h(\mathbf{X}_A|\mathbf{Y}_B)) = (n_A - \min(n_A, n_B))(m_A - n_A) \tag{121}$$

which differs from (29). The analysis of (30) is still valid here. So, it follows from (13), (121) and (30) that

$$\begin{aligned} DoF(h(\mathcal{X}|\mathcal{Y})) &= (n_A - \min(n_A, n_B))(m_A - n_A) \\ &\quad + n_A n_B(1 - \delta_{|\rho|-1}) \end{aligned} \tag{122}$$

which differs from (31).

2) Analysis of $h(\mathcal{X}|\mathcal{Z})$: For the first term in (32), which is similar to (121), we have

$$DoF(h(\mathbf{X}_A|\mathbf{Y}_{E,A})) = (n_A - \min(n_A, n_E))(m_A - n_A) \tag{123}$$

which differs from (36). For the second term in (32), we now refer to (37). Similar to (120), we have

$$DoF(h(\mathbf{Y}_{E,B})) = n_E n_B + \min(n_B, n_E)(m_B - n_B) \tag{124}$$

which differs from (38), and

$$\begin{aligned} DoF(h(\mathbf{Y}_A, \mathbf{Y}_{E,B})) &= (n_A + n_E)n_B \\ &\quad + \min(n_B, n_A + n_E)(m_B - n_B) \end{aligned} \tag{125}$$

which differs from (39). Therefore, (37) implies

$$\begin{aligned} DoF(h(\mathbf{Y}_A|\mathbf{Y}_{E,B})) &= n_A n_B \\ &\quad + \min(n_A, (n_B - n_E)^+)(m_B - n_B) \end{aligned} \tag{126}$$

which differs from (41). Finally, (32), (123) and (126) imply

$$\begin{aligned} DoF(h(\mathcal{X}|\mathcal{Z})) &= (n_A - \min(n_A, n_E))(m_A - n_A) + n_A n_B \\ &\quad + \min(n_A, (n_B - n_E)^+)(m_B - n_B) \end{aligned} \tag{127}$$

which differs from (42).

3) Analysis of $h(\mathcal{X}|\mathcal{Y}, \mathcal{Z})$: We now refer to the first term in (43). Similar to (123), we have

$$\begin{aligned} &DoF(h(\mathbf{X}_A|\mathbf{Y}_B, \mathbf{Y}_{E,A})) \\ &\quad = (n_A - \min(n_A, n_E + n_B))(m_A - n_A) \end{aligned} \tag{128}$$

which differs from (47). The DoF of the second term in (43) is given by (30). Therefore, we have

$$\begin{aligned} DoF(h(\mathcal{X}|\mathcal{Y}, \mathcal{Z})) &= n_A n_B(1 - \delta_{|\rho|-1}) \\ &\quad + (n_A - \min(n_A, n_E + n_B))(m_A - n_A) \end{aligned} \tag{129}$$

which differs from (48).

4) DoF of C_S: It follows from (122), (127) and (129) that

$$\begin{aligned} DoF(C_A) &= DoF(\mathcal{X}|\mathcal{Z}) - DoF(\mathcal{X}|\mathcal{Y}) \\ &= (\min(n_A, n_B) - \min(n_A, n_E))(m_A - n_A) \\ &\quad + \min(n_A, (n_B - n_E)^+)(m_B - n_B) + n_A n_B \delta_{|\rho|-1}, \end{aligned} \tag{130}$$

$$\begin{aligned} DoF(C_Z) &= DoF(\mathcal{X}|\mathcal{Z}) - DoF(\mathcal{X}|\mathcal{Y}, \mathcal{Z}) \\ &= (\min(n_A, n_E + n_B) - \min(n_A, n_E))(m_A - n_A) \\ &\quad + \min(n_A, (n_B - n_E)^+)(m_B - n_B) + n_A n_B \delta_{|\rho|-1}. \end{aligned} \tag{131}$$

We see that if $n_A \le n_B$, then $DoF(C_Z) = DoF(C_A)$. Furthermore, (131) can be rewritten as

$$\begin{aligned} DoF(C_Z) &= \min(n_B, (n_A - n_E)^+)(m_A - n_A) \\ &\quad + \min(n_A, (n_B - n_E)^+)(m_B - n_B) + n_A n_B \delta_{|\rho|-1} \end{aligned} \tag{132}$$

which is invariant to the exchange of "A" and "B". So we have $DoF(C_S) = DoF(C_Z) = \max(DoF(C_A), DoF(C_B))$.

Referring to Theorem 1 or (7), one can verify that

$$\begin{aligned} b_{A,B} - n_A n_B &= \begin{cases} 0, & n_E \ge n_A, \\ -n_A(n_A - n_E), & n_E < n_A \le n_B + n_E, \\ -n_A n_B, & n_A > n_B + n_E \end{cases} \\ &= -n_A \min(n_B, (n_A - n_E)^+) \end{aligned} \tag{133}$$

and similarly $b_{B,A} - n_A n_B = -n_B \min(n_A, (n_B - n_E)^+)$. Then it follows that (132) is identical to (7). ■

XI. Analysis of [5]

In [5], Alice has $n_A > 1$ antennas and Bob has one. For each channel coherent period, there are multiple channel probing sessions. In the k-th session, Alice selects the i_k-th antenna randomly and sends a sequence of random symbols $\sqrt{P}a_{k,l}$ with $1 \le l \le m_A$ to Bob over a subcarrier, and Bob in return sends a public pilot $\sqrt{P}$ to the i_k-th antenna of Alice. Here $1 \le k \le K$ with $K \ge n_A$. The signals received

by Bob, Alice and Eve during the k-th session can be written as $y_{B,k,l} = \sqrt{P}h_{i_k}a_{k,l} + w_{B,k,l}$, $y_{A,k} = \sqrt{P}h_{i_k} + w_{A,k}$, $\mathbf{y}_{E,A,k,l} = \sqrt{P}\mathbf{g}_{A,i_k}a_{k,l} + \mathbf{w}_{E,A,k,l}$ and $\mathbf{y}_{E,B,k} = \sqrt{P}\mathbf{g}_B + \mathbf{w}_{E,B,k}$. Here $\mathbf{g}_{A,i_k}$ is the channel vector from the i_k-th antenna of Alice to Eve, and $\mathbf{g}_B$ is the channel vector from Bob to Eve. The meanings of other notations are obvious. We will assume that all random symbols $\{a_{k,l}\}$, the complex scalars of all channel gains and all complex noise elements are i.i.d. $\mathcal{CN}(0,1)$.

The data sets available at Alice, Bob and Eve (for each subcarrier and each coherent period) are respectively $\mathcal{X}'' = \{a_{k,l}, y_{A,k}, \forall(k,l)\}$, $\mathcal{Y}'' = \{y_{B,k,l}, \forall(k,l)\}$, and $\mathcal{Z}'' = \{\mathbf{y}_{E,A,k,l}, \mathbf{y}_{E,B,k}, \forall(k,l)\}$. It is easy to verify that $DoF(h(\mathcal{Y}''|\mathcal{X}'')) = 0$ and hence $DoF(h(\mathcal{Y}''|\mathcal{X}'', \mathcal{Z}'')) = 0$. Then the secret key capacity C_S'' based on the above model satisfies

$$DoF(C_S'') = DoF(h(\mathcal{Y}''|\mathcal{Z}'')). \tag{134}$$

We know

$$\begin{aligned} h(\mathcal{Y}''|\mathcal{Z}'') &= h(y_{B,k,l}, \forall(k,l)|\mathbf{y}_{E,A,k,l}, \mathbf{y}_{E,B,k}, \forall(k,l)) \\ &= h(y_{B,k,l}, \forall(k,l)|\mathbf{y}_{E,A,k,l}, \forall(k,l)). \end{aligned} \tag{135}$$

Let $\mathcal{A} = \{\alpha_1, \ldots, \alpha_{n_A}\}$ consist of (any) n_A elements from $\{a_{k,l}, \forall(k,l)\}$ that are transmitted from n_A distinct antennas of Alice (i.e., antenna 1 to antenna n_A), and $\bar{\mathcal{A}}$ consist of all other elements from $\{a_{k,l}, \forall(k,l)\}$. Here we assume that K is large enough so that every antenna of Alice has been chosen at least once. Also let $\mathcal{B}$ consist of the entries from $\{y_{B,k,l}, \forall(k,l)\}$ corresponding to $\mathcal{A}$, and $\bar{\mathcal{B}}$ consist of all other entries from $\{y_{B,k,l}, \forall(k,l)\}$. It follows that

$$h(\mathcal{Y}''|\mathcal{Z}'') = h(\mathcal{B}|\mathbf{y}_{E,A,k,l}, \forall(k,l)) + h(\bar{\mathcal{B}}|\mathcal{B}, \mathbf{y}_{E,A,k,l}, \forall(k,l)). \tag{136}$$

Note that at high power P, $\mathcal{B} \approx \{\sqrt{P}\alpha_1 h_1, \ldots, \sqrt{P}\alpha_{n_A}h_{n_A}\}$ where $\{h_1, \ldots, h_{n_A}\}$ are independent of $\mathbf{y}_{E,A,k,l}, \forall(k,l)$. Hence

$$DoF(h(\mathcal{B}|\mathbf{y}_{E,A,k,l}, \forall(k,l))) = n_A. \tag{137}$$

Also at high power, $\mathbf{y}_{E,A,k,l} \approx \sqrt{P}\mathbf{g}_{A,k,l}a_{k,l}$, and every entry of $\bar{\mathcal{B}}$ has a form approximately equal to $\sqrt{P}h_{i_k}a_{k,l} = \sqrt{P}h_{i_k}\alpha_{i_k}\frac{a_{k,l}}{\alpha_{i_k}}$. Note that $\sqrt{P}h_{i_k}\alpha_{i_k}$ is among the entries in $\mathcal{B}$, and $\frac{a_{k,l}}{\alpha_{i_k}}$ is approximately the ratio of one element in $\mathbf{y}_{E,A,k,l} \approx \sqrt{P}\mathbf{g}_{A,k,l}a_{k,l}$ over a corresponding element in $\mathbf{y}_{E,A,k',l'} \approx \sqrt{P}\mathbf{g}_{A,k',l'}a_{k',l'}$ where $a_{k',l'} = \alpha_{i_k}$. So, we have

$$DoF(h(\bar{\mathcal{B}}|\mathcal{B}, \mathbf{y}_{E,A,k,l}, \forall(k,l))) = 0. \tag{138}$$

Therefore, for all $n_E \geq 1$,

$$DoF(C_S'') = DoF(h(\mathcal{Y}''|\mathcal{Z}'')) = n_A. \tag{139}$$

This result says that in terms of DoF of secret key capacity, the channel probing scheme proposed in [5] has the same performance as the conventional scheme using public pilots from both Alice and Bob. The random selection of antennas at Alice adds some computational complexity for Eve but does not increase the DoF of secret key capacity.

In the next section, we show a special form of the proposed GCP and GPP, which has a far more superior DoF of secret key capacity. Provided $n_E < n_A$, this special form requires no channel reciprocity but has an increasing DoF of secret key capacity as the number of transmissions per coherence period increases.

XII. Further Discussions

In this section, we discuss a special case of the proposed GCP and GPP, and reveal additional insights into Theorems 1, 2 and 3. We will also provide some remarks on potential applications of GCP and GPP.

A. GCP and GPP With $m_A > n_A$ and $m_B = 0$

We now consider the case where there is no channel reciprocity to exploit. We also let GCP involve only the transmission from Alice to Bob, and write $\mathbf{X}_A = [\mathbf{X}_{A,\gamma}, \mathbf{X}_{A,\tau}]$ where $\mathbf{X}_{A,\gamma}$ has the dimension $n_A \times n_A$ and $\mathbf{X}_{A,\tau}$ has the dimension $n_A \times (m_A - n_A)$. (We will see that $\mathbf{X}_{A,\gamma}$ can be public without affecting the DoF of a desired secrecy.) Then the signals received by Bob and Eve can be written as

$$\mathbf{Y}_B = [\mathbf{Y}_{B,\gamma}, \mathbf{Y}_{B,\tau}], \tag{140}$$

$$\mathbf{Y}_{E,A} = [\mathbf{Y}_{E,A,\gamma}, \mathbf{Y}_{E,A,\tau}], \tag{141}$$

where $\mathbf{Y}_{B,i} = \mathbf{H}_{B,A}\mathbf{X}_{A,i} + \mathbf{W}_{B,i}$ and $\mathbf{Y}_{E,A,i} = \mathbf{G}_A\mathbf{X}_{A,i} + \mathbf{W}_{E,A,i}$ with $i = \gamma, \tau$. Here we choose the notations of "γ and τ" to be consistent with the discussions in Section VII-C.

For GPP, we let Bob transmit via a public channel $\mathbf{Y}'_B = [\mathbf{Y}_{B,\gamma}, \mathbf{Y}'_{B,\tau}]$ with $\mathbf{Y}'_{B,\tau} = \mathbf{Y}_{B,\tau} + \mathbf{Q}_\tau$ and $\mathbf{Q}_\tau$ being an $n_B \times (m_A - n_A)$ matrix of random symbols of secret information. This is a simplified iSAT from that shown before Theorem 2.

B. Secrecy of $\mathbf{Q}_\tau$ Against Eve

To understand the (most conservative) secrecy of the above scheme, we assume that Eve knows

$$\mathcal{Z}_s \doteq \{\mathbf{H}_{B,A}, \mathbf{G}_A, \bar{\mathbf{Y}}_{E,A,\gamma}, \bar{\mathbf{Y}}_{E,A,\tau}, \bar{\mathbf{Y}}_{B,\gamma}, \bar{\mathbf{Y}}'_{B,\tau}\}. \tag{142}$$

Here $\bar{\mathbf{Y}}_{E,A,\gamma}, \bar{\mathbf{Y}}_{E,A,\tau}, \bar{\mathbf{Y}}_{B,\gamma}$ and $\bar{\mathbf{Y}}'_{B,\tau}$ are the noiseless versions of $\mathbf{Y}_{E,A,\gamma}$, $\mathbf{Y}_{E,A,\tau}$, $\mathbf{Y}_{B,\gamma}$ and $\mathbf{Y}'_{B,\tau}$. Namely, $\bar{\mathbf{Y}}_{E,A,\gamma} = \mathbf{G}_A\mathbf{X}_{A,\gamma}$, $\bar{\mathbf{Y}}_{E,A,\tau} = \mathbf{G}_A\mathbf{X}_{A,\tau}$, $\bar{\mathbf{Y}}_{B,\gamma} = \mathbf{H}_{B,A}\mathbf{X}_{A,\gamma}$ and $\bar{\mathbf{Y}}'_{B,\tau} = \mathbf{H}_{B,A}\mathbf{X}_{A,\tau} + \mathbf{Q}_\tau$.

We are interested in the secrecy measured by $DoF(h(\mathbf{Q}_\tau|\mathcal{Z}_s))$. Since $\mathbf{X}_{A,\gamma}$ is independent of $\mathbf{X}_{A,\tau}$, we see that $\bar{\mathbf{Y}}_{E,A,\gamma}$ and $\bar{\mathbf{Y}}_{B,\gamma}$ are independent of $\mathbf{Q}_\tau$ given $\mathbf{H}_{B,A}$ and $\mathbf{G}_A$. But the relationship between $\bar{\mathbf{Y}}_{E,A,\tau}$, $\bar{\mathbf{Y}}'_{B,\tau}$ and $\mathbf{Q}_\tau$ is governed by

$$\mathbf{Y}_E \doteq \begin{bmatrix} \bar{\mathbf{Y}}_{E,A,\tau} \\ \bar{\mathbf{Y}}'_{B,\tau} \end{bmatrix} = \begin{bmatrix} \mathbf{G}_A & \mathbf{0} \\ \mathbf{H}_{B,A} & \mathbf{I}_{n_B} \end{bmatrix} \begin{bmatrix} \mathbf{X}_{A,\tau} \\ \mathbf{Q}_\tau \end{bmatrix} \tag{143}$$

where both $\mathbf{X}_{A,\tau}$ and $\mathbf{Q}_\tau$ are unknown to Eve.

Theorem 4: Let $\mathbf{X}_{A,\tau}$ and $\mathbf{Q}_\tau$ consist of i.i.d. $\mathcal{CN}(0,P)$ elements. The necessary and sufficient condition for $DoF(h(\mathbf{Q}_\tau|\mathcal{Z}_s)) = \xi(m_A - n_A)$ with a positive integer $\xi > 0$ (relative to P) is that $row(\mathbf{H}_{B,A}) \not\subset row(\mathbf{G}_A)$ or equivalently $null(\mathbf{G}_A) \not\subset null(\mathbf{H}_{B,A})$.

Proof: If $row(\mathbf{H}_{B,A}) \subset row(\mathbf{G}_A)$, then there is a matrix $\mathbf{T}$ such that $\mathbf{H}_{B,A} = \mathbf{T}\mathbf{G}_A$ and hence $\mathbf{Q}_\tau = \bar{\mathbf{Y}}'_{B,\tau} - \mathbf{T}\bar{\mathbf{Y}}_{E,A,\tau}$. In this case, $DoF(h(\mathbf{Q}_\tau|\mathcal{Z}_s)) = 0$, i.e., $\xi = 0$. If $null(\mathbf{G}_A) \subset null(\mathbf{H}_{B,A})$, $\bar{\mathbf{Y}}_{E,A,\tau}$ yields $\hat{\mathbf{X}}_{A,\tau} \doteq \mathbf{G}_A^\dagger\bar{\mathbf{Y}}_{E,A,\tau}$ such that $\mathbf{X}_{A,\tau} = \hat{\mathbf{X}}_{A,\tau} + \mathbf{N}_G\mathbf{X}_{a,\tau}$ where $\mathbf{N}_G^H\mathbf{N}_G = \mathbf{I}$, $range(\mathbf{N}_G) =$

$null(\mathbf{G}_A)$ and $\mathbf{X}_{a,\tau}$ is free. And in this case $\bar{\mathbf{Y}}'_{B,\tau} = \mathbf{H}_{B,A}\hat{\mathbf{X}}_{A,\tau} + \mathbf{Q}_\tau$ and hence $DoF(h(\mathbf{Q}_\tau|\mathcal{Z}_s)) = 0$.

If $row(\mathbf{H}_{B,A}) \not\subset row(\mathbf{G}_A)$, there is a matrix $\mathbf{T}_E$ such that

$$\mathbf{T}_E\mathbf{Y}_E = \begin{bmatrix} \mathbf{G}_A & \mathbf{0}_{n_E\times n_a} & \mathbf{0}_{n_E\times n_b} \\ \mathbf{0}_{n_a\times n_A} & \mathbf{I}_{n_a} & \mathbf{T}_b \\ \mathbf{H}_{b,A} & \mathbf{0}_{n_b\times n_a} & \mathbf{I}_{n_b} \end{bmatrix} \begin{bmatrix} \mathbf{X}_{A,\tau} \\ \mathbf{Q}_{\tau,a} \\ \mathbf{Q}_{\tau,b} \end{bmatrix} \quad (144)$$

where $n_a + n_b = n_B$, the n_b rows of $\mathbf{H}_{b,A}$ are a subset of n'_b independent rows from $\mathbf{H}_{B,A}$, no row of $\mathbf{H}_{b,A}$ belongs to $row(\mathbf{G}_A)$, $n_b \le n'_b \le n_B$, and $[\mathbf{Q}^T_{\tau,a}, \mathbf{Q}^T_{\tau,b}] = (\mathbf{P}_Q\mathbf{Q}_\tau)^T$ with $\mathbf{P}_Q$ being a permutation matrix. Here we see that $\mathbf{Q}_{\tau,a} + \mathbf{T}_b\mathbf{Q}_{\tau,b}$ is exposed but $\mathbf{Q}_{\tau,b}$ is still protected. More specifically, conditional on $\mathcal{Z}_s$, $\mathbf{X}_{A,\tau} = \mathbf{G}^\dagger_A\mathbf{Y}_{E,T,1} + \mathbf{N}_G\mathbf{X}_{A,G}$ where $\mathbf{Y}_{E,T,1}$ is the first n_E rows of $\mathbf{T}_E\mathbf{Y}_E$, $range(\mathbf{N}_G) = null(\mathbf{G}_A)$, $\mathbf{N}^H_G\mathbf{N}_G = \mathbf{I}$ and $\mathbf{X}_{A,G} = \mathbf{N}^H_G\mathbf{X}_{A,\tau}$. Note that $\mathbf{X}_{A,G}$ is not observable from $\mathbf{Y}_{E,T,1}$. Furthermore, given the last n_b rows of $\mathbf{T}_E\mathbf{Y}_E$, each of the $m_A - n_A$ independent columns of $\mathbf{Q}_{\tau,b}$ has the PDF $\mathcal{CN}(*, P\mathbf{H}_{b,A}\mathbf{N}_G\mathbf{N}^H_G\mathbf{H}^H_{b,A})$ where $rank(\mathbf{H}_{b,A}\mathbf{N}_G) = n_b$. Also note that the middle n_a rows of $\mathbf{T}_E\mathbf{Y}_E$ are independent of $\mathbf{X}_{A,\tau}$ and $\mathbf{Q}_{\tau,b}$. Hence, $DoF(h(\mathbf{Q}_\tau|\mathcal{Z}_s)) = DoF(h(\mathbf{Q}_{\tau,b}|\mathcal{Z}_s)) = n_b(m_A - n_A)$. (Note that the singularity in $h(\mathbf{Q}_\tau|\mathcal{Z}_s)$ caused by a known entry in $\mathbf{Q}_\tau$ does not affect $DoF(h(\mathbf{Q}_\tau|\mathcal{Z}_s))$ relative to power P. This singularity would disappear if the noise in $\mathbf{Y}'_{B,\tau}$ is considered.) ■

Next we assume that $\mathbf{G}_A$ and $\mathbf{H}_{B,A}$ consist of elements that are realizations of i.i.d. $\mathcal{CN}(0,1)$ random variables. We will use the rank conditions that are met with probability one.

Corollary 3: With probability one,

$$DoF(h(\mathbf{Q}_\tau|\mathcal{Z}_s)) = \min(n_B, (n_A - n_E)^+)(m_A - n_A) \quad (145)$$

which equals the first term in (1) or equivalently $a_{A,B} + b_{A,B} - n_An_B$ in (7).

Proof: If $n_E \ge n_A$, then $row(\mathbf{H}_{B,A}) \subset row(\mathbf{G}_A) = \mathcal{C}^{n_A}$ with probability one, and hence $DoF(h(\mathbf{Q}_\tau|\mathcal{Z}_s)) = 0$. If $n_A > n_E$ and $n_B \le n_A - n_E$, then $\begin{bmatrix} \mathbf{G}_A \\ \mathbf{H}_{B,A} \end{bmatrix}$ is a square or wide matrix. In this case, with probability one, no row of $\mathbf{H}_{B,A}$ belongs to $row(\mathbf{G}_A)$ and hence $DoF(h(\mathbf{Q}_\tau|\mathcal{Z}_s)) = n_B(m_A - n_A)$. If $n_A > n_E$ and $n_B > n_A - n_E$, then with probability one, there is a matrix $\mathbf{T}_E$ such that (144) holds where $n_a = n_E + n_B - n_A$, $n_b = n_A - n_E$, and $\mathbf{H}_{b,A}$ has the rank n_b and contains no row that belongs to $row(\mathbf{G}_A)$, and none of $n_A - n_E$ independent null vectors of $\mathbf{G}_A$ belongs to $null(\mathbf{H}_{B,A})$. In this case, $DoF(h(\mathbf{Q}_\tau|\mathcal{Z}_s)) = DoF(h(\mathbf{Q}_{\tau,b}|\mathcal{Z}_s)) = (n_A - n_E)(m_A - n_A)$. ■

C. Estimation of $\mathbf{Q}_\tau$ at Alice

Given $\mathbf{X}_{A,\gamma}$ and $\mathbf{Y}_{B,\gamma} = \mathbf{H}_{B,A}\mathbf{X}_{A,\gamma} + \mathbf{W}_{B,\gamma}$, Alice can find an estimate of $\mathbf{H}_{B,A}$. In fact, if $\mathbf{X}_{A,\gamma}$ is public, Bob could also estimate $\mathbf{H}_{B,A}$ and then send $\mathbf{H}_{B,A}$ along with $\mathbf{Y}'_{B,\tau}$. Theorem 4 and Corollary 3 assume that Eve knows $\mathbf{H}_{B,A}$.

With knowledge of $\mathbf{X}_{A,\tau}$, $\mathbf{Y}'_{B,\tau}$ and an estimate $\hat{\mathbf{H}}_{B,A}$ of $\mathbf{H}_{B,A}$, Alice can compute

$$\hat{\mathbf{Q}}_\tau = \mathbf{Y}'_{B,\tau} - \hat{\mathbf{H}}_{B,A}\mathbf{X}_{A,\tau} \approx \mathbf{Q}_\tau + \mathbf{W}_{B,\tau}. \quad (146)$$

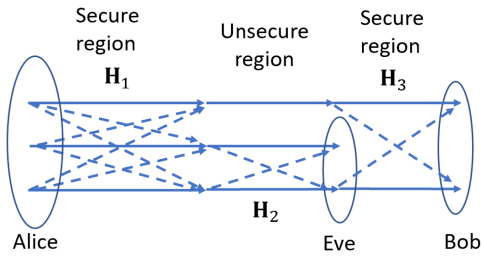

Fig. 2. Wireline channels where GCP and GPP could be applied if $range(\mathbf{H}^T_{B,A}) \not\subset range(\mathbf{G}^T_A)$ with $\mathbf{H}_{B,A} = \mathbf{H}_3 diag(1, \mathbf{H}_2)\mathbf{H}_1$ and $\mathbf{G}_A = \mathbf{H}_2\mathbf{H}_1$. Here three strongly coupled wires originated from Alice traverse separately over a wide unsecured field while two of them are wiretapped by Eve and two of them are eventually connected to Bob. A randomized $\mathbf{H}_1$ could be artificially generated by Alice even if $\mathbf{H}_2$ and $\mathbf{H}_3$ become selection matrices due to good insulation between wires.

where the approximation holds if the error in $\hat{\mathbf{H}}_{B,A}$ is negligible due to an extra large power in $\mathbf{X}_{A,\gamma}$. We see that (146) is equivalent to a standard additive white Gaussian noise (AWGN) channel with input $\mathbf{Q}_\tau$ and output $\hat{\mathbf{Q}}_\tau$. Bob can apply a conventional method to encode secret information into $\mathbf{Q}_\tau$ to allow Alice to detect the secret information reliably. This secret information can be used as a secret key.

If the public channel used for GPP is replaced by a conventional wireless channel (such as the reverse channel of $\mathbf{H}_{B,A}$ in the case of no other available channel between Alice and Bob), the estimate and detection problem at Alice can be handled with no major technical hurdles. The only difference would be additional noise caused in the transmission from Bob to Alice.

D. Applications to Wireline Channels

Theorem 4 also suggests a feasibility of applying GCP and GPP for SKG from wireline channels. We see that the crucial condition for a desired secrecy DoF is that the row space of the channel $\mathbf{H}_{B,A}$ from Alice to Bob does not belong the row space of the channel $\mathbf{G}_A$ from Alice to Eve. To ensure that such a condition is met in wireline setting (such as twisted copper wires), one could construct a network where the observable channels by Bob are not a subset of the observable channels by Eve. For example, see Fig. 2.

E. Applications to mmW Channels

A large number of transmit antennas (a large n_A) is feasible for millimeter-wave (mmW) systems. But for mmW applications, there are typically strong line-of-sight paths which could destroy the sufficient and necessary condition required on the channel matrices as shown in Theorem 4. Further research in this direction is required. One way to help to meet the required condition could be the use of artificial scatterers (or "electromagnetic camouflage") around Bob during GCP.

F. Diversifying the Channels for GCP and GPP

Two very different channels can be used for GCP and GPP respectively. The chance for Eve to have the full accesses to both channels could be very small if Alice and Bob have multiple channels between them to choose from. For example, if GCP is based on a wireless MIMO channel and GPP is based on a

wireline channel, it would take a very sophisticated Eve to have a high quality access to both.

XIII. Conclusion

This work was in part inspired by those shown in [4] and [5] although our analysis shows that in terms of degree of freedom (DoF) of secret key capacity (SKC), none of the prior works achieves what the authors intended to achieve. This paper has presented a generalized channel probing (GCP) method and a generalized pre-processing (GPP) method for SKG from a MIMO channel with or without reciprocity. It is shown that the SKC-DoF of GCP is given by (1) and GPP does not result in any loss of SKC-DoF unless additional constraints are used for reduced computational complexity. It is also shown that by embedding public pilots in the transmissions during GCP, there is still no loss of SKC-DoF while the computational complexity of GPP is substantially reduced. It is yet unclear whether the public pilots affect the secondary measure of SKC. For GCP with fully randomized transmissions, the corresponding GPP needs to solve a non-convex computational problem. It is yet unclear whether this problem can be solved much more efficiently than shown in this paper. While GCP and GPP in this paper are readily applicable to half-duplex radios where the MIMO channel between users may or may not be reciprocal, future research should also consider the use of full-duplex radio for SKG. For a network of collaborative full-duplex radio nodes, a positive reciprocity-independent SKC-DoF is available even if Eve has an unlimited number of antennas (including the case of Eve having more antennas than both Alice and Bob), e.g., see [15], [16]. How to design a good (i.e., SKC-DoF preserving) pre-processing method for the data sets collected by two or more full-duplex radio nodes remains an open problem.

Acknowledgment

The views and conclusions contained in this document are those of the author and should not be interpreted as representing the official policies, either expressed or implied, of the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation herein.

References

[1] J. Zhang, G. Li, A. Marshall, A. Hu, and L. Hanzo, "A new frontier for IoT security emerging from three decades of key generation relying on wireless channels," *IEEE Access*, vol. 8, pp. 138406–138446, 2020.

[2] C. Huth, R. Guillaume, T. Strohm, P. Duplys, and I. A. Samuel, "Information reconciliation schemes in physical-layer security: A survey," *Comput. Netw.*, vol. 109, pp. 84–104, 2016.

[3] R. Wilson, D. Tse, and R. A. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE Trans. Inf. Forensics Secur.*, vol. 2, no. 3, pp. 364–375, Sep. 2007.

[4] N. Aldaghri and H. Mahdavifar, "Physical layer secret key generation in static environments," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 2692–2705, 2020.

[5] G. Li, H. Yang, J. Zhang, H. Liu, and A. Hu, "Fast and secure key generation with channel obfuscation in slowly varying environments," in *Proc. IEEE Conf. Comput. Commun.*, 2022, pp. 1–10.

[6] S. S. Pradhan and K. Ramchandran, "Distributed source coding using syndromes (DISCUS): Design and construction," *IEEE Trans. Inf. Theory*, vol. 49, no. 3, pp. 626–643, Mar. 2003.

[7] J. W. Wallace and R. K. Sharma, "Automatic secret keys from reciprocal MIMO wireless channels: Measurement and analysis," *IEEE Trans. Inf. Forensics Secur.*, vol. 5, no. 3, pp. 381–392, Sep. 2010.

[8] A. Maksud and Y. Hua, "Secret key generation by continuous encryption before quantization," *IEEE Signal Process. Lett.*, vol. 29, pp. 1497–1501, 2022.

[9] Y. Hua and A. Maksud, "Continuous encryption functions for security over networks," *Signal Process.*, vol. 203, pp. 1–15, 2023.

[10] Y. Dodis, B. Kanukurthi, J. Katz, L. Reyzin, and A. Smith, "Robust fuzzy extractors and authenticated key agreement from close secrets," *IEEE Trans. Inf. Theory*, vol. 58, no 9., pp. 6207–6222, Sep. 2012.

[11] A. A. Nasir, S. Durrani, H. Mehrpouyan, S. D. Blostein, and R. A. Kennedy, "Timing and carrier synchronization in wireless communication systems: A survey and classification of research in the last 5 years," *EURASIP J. Wireless Commun. Netw.*, vol. 2016, 2016, Art. no. 180.

[12] Y. Hua, "Anti-eavesdopping channel estimation using multi-antenna half-duplex radios," in *Proc. IEEE Mil. Commun. Conf.*, San Diego, CA, 2021, pp. 910–915.

[13] T.-Y. Liu, P. Mukherjee, S. Ulukus, S.-C. Lin, and Y.-W. P. Hong, "Secure degrees of freedom of MIMO Rayleigh block fading wiretap channels with no CSI anywhere," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2655–2669, May 2015.

[14] M. Zorgui, Z. Rezki, B. Alomair, and M.-S. Alouini, "The diversity-multiplexing tradeoff of secret-key agreement over multiple antenna channels," *IEEE Trans. Wireless Commun.*, vol. 15. no 2, pp. 1562–1574, Feb. 2016.

[15] Y. Hua, "Advanced properties of full-duplex radio for securing wireless network," *IEEE Trans. Signal Process.*, vol. 67, no 1, pp. 120–135, Jan. 2019.

[16] S. Wu and Y. Hua, "Total secrecy from anti-eavesdropping channel estimation," *IEEE Trans. Signal Process.*, vol. 70, pp. 1088–1103, 2022.

[17] M. Bloch and J. Barros, *Physical-Layer Security*. Cambridge, MA, USA: Cambridge Univ. Press, 2011.

[18] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[19] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd. Hoboken, NJ, USA:Wiley, 2006.

Yingbo Hua (Fellow, IEEE) received the bachelor's degree from Southeast University, Nanjing, China, in 1982, and the Ph.D. degree from Syracuse University, Syracuse, NY, USA, in 1988. He held a Faculty position with the University of Melbourne, Parkville VIC, Australia, during 1990–2001, and has been a Professor with the University of California at Riverside, Riverside, CA, USA, since 2001. He has authored or coauthored more than 350 articles in the field of signal processing for sensing, communications and security. He has advised more than 50 Ph.D. students, visiting Ph.D. students, postdoctoral fellows and visiting scholars. He was for many years, the editor and/or guest editor for IEEE Transactions on Signal Processing, IEEE Signal Processing Letters, *EURASIPs Signal Processing*, *IEEE Signal Processing Magazine*, IEEE Journal of Selected Areas in Communications, and IEEE Transactions on Signal and Information Processing over Networks. He was for many years an elected member on IEEE SPS Technical Committees for Signal Processing for Communications, and Sensor Array and Multichannel Processing. He was the Chair of Steering Committee for IEEE Wireless Communications Letters, January 2020–December 2021, and Chair of IEEE GlobalSIP Symposium on Signal Processing for Wireless Network Security, November 2018. He is a Fellow of AAAS.