Optimality of the Proper Gaussian Signal in Complex MIMO Wiretap Channels

Yong Dong, Member, IEEE, Yinfei Xu, Member, IEEE, Tong Zhang, Member, IEEE, and Yili Xia, Member, IEEE

Abstract—The multiple-input multiple-output (MIMO) wiretap channel (WTC) serves as a fundamental model for exploring information-theoretic secrecy in wireless communication systems, involving a transmitter, a legitimate user, and an eavesdropper. This paper investigates the optimality of proper complex signals in complex WTCs. Our primary contribution lies in the derivation of a determinant inequality, which establishes that the secrecy rate of degraded complex MIMO WTCs is maximized when the signal is proper, meaning that its pseudo-covariance matrix is a zero matrix. Remarkably, we extend this result beyond the degraded scenario to the general complex WTC by leveraging a min-max reformulation of the secrecy capacity. Thus, we demonstrate that focusing on proper signals is sufficient when examining the secrecy capacity of the complex WTC. Overall, this work highlights the significance of the determinant inequality we derive and its implications for optimizing secrecy rates in the complex WTC.

Index Terms—Matrix inequality, proper and improper signals, secrecy capacity, wiretap channel.

I. INTRODUCTION

THE broadcast nature of wireless communications has underscored the significance of ensuring secure communication channels for many years. Traditionally, communication security is achieved through cryptographic techniques to achieve computational security at an upper layer. However, the effectiveness of such security measures hinges on a comparison between the complexity of attacking the system and the computational power available to the attacker, subject to specific conditions. In contrast, physical layer security at the bottom level was proposed by Shannon to ensure secure communications regardless of the attacker’s computing power [1].

In this paper, we consider complex Gaussian signals for wiretap channels (WTCs), which is a fundamental model in information-theoretic security. Despite the significance of WTCs, a closed-form expression for the secrecy capacity of MIMO Gaussian WTCs has not been established since their introduction by Wyner in [2], and the extension to the Gaussian case in [3]. Previous works, such as [4], [5], and [6], have addressed the characterization of secrecy capacity for MIMO WTCs as a maximization problem. Specifically, [4], [5] focused on the complex WTC, while [6] examined the real WTC. Notably, the optimal transmit covariance matrix has been derived for the MISO WTC [7], [8], [9] and certain special cases of MIMO WTCs, such as the strictly degraded Gaussian MIMO WTC with sufficiently large power [10]. Furthermore, [11] presented a characterization of the optimal covariance matrix with an arbitrary number of antennas, assuming it is full-rank. Recent efforts have introduced optimization methods for obtaining numerical results in the context of Gaussian MIMO WTCs. For instance, [12] proposed a difference of convex functions algorithm (DCA) for calculating the secrecy rate of WTCs. Some other numerical methods are based on the min-max (convex-concave) reformulation of the secrecy capacity for Gaussian MIMO WTCs [10], [13], [14], [15]. Building upon these works, [16] introduced an accelerated difference of convex functions algorithm (ADCA) and a partial best response algorithm (PBRA). Additionally, the multiple access wiretap channel (MAC-WTC) has recently gained attention, although the capacity of MAC-WTCs remains unknown [17]. Nevertheless, numerical algorithms have been proposed in [18], [19] and are worth considering. It is important to note that, for a general complex-valued signal, it can be either proper or improper [20]; however, all the aforementioned works have exclusively focused on proper transmit signals.

Throughout the years, a widely held assumption has been that complex signals employed in complex channels are proper, meaning that the transmitted signal is uncorrelated with its complex conjugate. This assumption offers the advantage of simplifying the calculation of channel capacity, as the computations and outcomes closely resemble those of real signals. Consequently, by leveraging existing results for real cases, it becomes easier to derive secrecy capacity for the proper scenario. Neeser et al. [21] further demonstrated that the differential entropy of a complex random vector, with a fixed correlation matrix, is maximized only when the vector is proper, Gaussian, and zero-mean. As a result, it has been proven that proper signals achieve capacity in point-to-point channels [22] and multiple access channels (MAC) [23, Lemma 1]. The optimality of proper Gaussian signals

Manuscript received 30 January 2023; revised 2 July 2023 and 11 September 2023; accepted 17 October 2023. Date of publication 28 November 2023; date of current version 7 December 2023. This work was supported in part by the National Natural Science Foundation of China under Grant 6237119, in part by the Zhi Shan Young Scholar Program of Southeast University, in part by the Fundamental Research Funds for the Central Universities under Grant 11623336, and in part by the Fundamental Research Funds for the Central Universities under Grant 2242022K30002. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Haijun Zhang. (Corresponding author: Yinfei Xu.)

Tong Zhang is with the College of Information Science and Technology, Jinan University, Guangzhou 510632, China (e-mail: zhang77@jnu.edu.cn), Digital Object Identifier 10.1109/TIFS.2023.3337719

Authorized licensed use limited to the terms of the applicable license agreement with IEEE. Restrictions apply.
has also been established in the Gaussian multiple-input multiple-output (MIMO) broadcast channel (BC) through the application of dirty paper coding (DPC) under a sum power constraint [24]. Furthermore, this optimality has been extended to the Gaussian MIMO BC with DPC under a sum covariance constraint [23]. Expanding on these findings, subsequent research has demonstrated that proper signals are optimal in the MIMO relay channel with partial decode-and-forward. The reformulation of this problem exhibits similarities to a sum rate maximization problem in a two-user MIMO BC. Consequently, the assumption of transmit signals being proper has become increasingly prevalent in theoretical analyses, particularly when the capacity-achieving distribution is proven to be Gaussian.

However, there are other scenarios where improper Gaussian signals outperform proper Gaussian signals with respect to channel capacities or achievable rates. Most of them are interference-dominant situations because the existence of interference plays the role as an improper noise, such as in the interference channel (IC) [25], [26], [27], [28] and in the cognitive network [29], [30]. It’s worth mentioning that although Neesser et al.’s result appears to guarantee that point-to-point channel achieves capacity with proper signals [21], if the additive Gaussian noise is improper, the optimal signal will become improper. In [26, Remark 1], it described heuristically that from the user k’s perspective in the IC, if interference is treated as noise, the user k essentially communicates over a point-to-point channel. However, the proper signal is strictly sub-optimal in this point-to-point channel, which is mainly because the noise containing interference can be improper if the transmitted signal is improper, so the analysis for the original point-to-point channel is no longer applicable here. Moreover, for the two-user BC with two private messages, it has been derived that every boundary point is achieved when at least one user employs the improper signal in [31].

For WTCs, although the legitimate user’s communication is point-to-point, the existence of an eavesdropper makes the secrecy capacity of the MIMO WTC also has the form of the difference of two logarithm-determinant functions, which is similar to the achievable rate for one specific user in the IC, where the improper signal can enlarge the achievable rate. On the other hand, we cannot directly assert that improper signals are superior since improper signals sometimes may bring no gains in the IC [25]. Therefore, in this paper, we manage to figure out whether the proper signal or the improper signal is optimal for the complex MIMO WTC. To demonstrate the optimality of the improper signal, previous studies have typically employed numerical algorithms to find an improper solution and establish its superiority over the proper signal [26], [30], [32], [33], [34]. However, when it comes to proving the optimality of the proper signal, numerical algorithms are not applicable due to the impracticality of exhaustively considering all possible improper signals and demonstrating their inferiority. In such cases, theoretical analyses become the only viable approach [21], [22], [23], with Fischer’s inequality [20, Result 2.2] being one of the crucial theoretical techniques. Inspired by Fischer’s inequality, we aim to establish a similar determinant inequality that will enable us to provide a conclusive proof. By leveraging this determinant inequality, we demonstrate that the proper signal is indeed optimal for achieving the secrecy capacity of complex WTCs.

It is worth mentioning that in practical communication schemes, the complex signals are usually assumed to be transmitted in Quadrature Amplitude Modulation (QAM), Orthogonal Frequency Division Multiplexing (OFDM) [35] modulation schemes and some other schemes involving transmission of information over orthogonal channels. This correspondence is facilitated by the direct mapping of in-phase and quadrature signals to the real and imaginary components of the complex signal. Improper Gaussian signals, distinguished by correlated real and imaginary parts, naturally emerge in communication systems due to gain imbalances and specific digital modulations like binary phase shift keying (BPSK) or Gaussian minimum shift keying (GMSK). Notably, improper signaling finds application in systems such as GSM (Global System for Mobile communication) [36], [37] and 3GPP (3rd Generation Partnership Project) [38]. In the field of information theory, the degrees of freedom (DoF) of ICs are different when employing proper and improper Gaussian signals. Actually, for the 3-user IC, the DoF is 1.5 with proper transmitted signals, while is 1.2 with the improper signals [39]. As a consequence, the debate regarding the optimality of proper versus improper Gaussian signals encompasses multiple facets. We focus on determining whether proper or improper Gaussian signals can attain superior data transmission rates. Most existing research supports the optimality of improper signals, particularly in Single-Input Single-Output (SISO) channels [25], [27], [31], [40], [41], [42], with numerical methods. In select Multiple-Input Multiple-Output (MIMO) channels, improper signaling’s optimality is also demonstrated through numerical computations [30], [33]. Conversely, evidence substantiating the optimality of proper signals is limited, as their optimality cannot be ascertained through numerical methods, as discussed in Section VI. Instead, the optimality of proper signals is proven through the convexity of the channel capacity [22] or its duality to a convex problem [23], [24].

A. Main Contributions

This paper establishes several results about the secrecy capacity of the complex MIMO WTC.

- This paper leverages the dependency of information measures on the distribution of random variables, rather than their specific values, to derive the achievable secrecy rate of a given Gaussian signal, expressed through an augmented covariance matrix. Moreover, it characterizes the secrecy capacity of WTC using general complex signals under a sum power constraint. This characterization involves maximizing achievable rates over the set of all possible augmented covariance matrices. Notably, our findings briefly demonstrate that previous works on the secrecy capacity of the complex WTC have not considered the possibility that improper signals may achieve superior secrecy rates. This paper derives a matrix determinant inequality by utilizing a simple conditional entropy inequality. This determinant inequality bears
resemblance to Fischer’s inequality and plays a crucial role in our proof, establishing that proper signals are capacity-achieving in the complex degraded WTC.

- This paper utilizes the min-max reformulation of the secrecy capacity of WTC, which is the minimization on the set of correlation matrices of two augmented noises and the maximization on the set of augmented covariance matrices of the transmitted signal. Then the result of the degraded WTC can be applied to the min-max reformulated expression and presents the secrecy capacity is achieved when the signal is proper. This paper represents the first demonstration of the optimality of proper signals within a non-convex setting, to the best of the authors’ knowledge.

B. Paper Organization and Notations

The rest of this paper is organized as follows. Section II starts with a brief review of the system model and the proper signal. Section III studies the secrecy capacity of the general WTC, which is expressed with the augmented covariance matrix. Section IV proposes a determinant inequality and proves that the proper signal can achieve the secrecy capacity. In Section V, the optimality of the proper signal for the general WTC is proved based on the result of degraded WTC and the min-max reformulation of the secrecy capacity. In section VI, we utilizes two algorithms in previous research to compare the maximum achievable rate for the proper signal and general complex signal. Finally, we conclude the paper in Section VII.

We adopt the following notations throughout the paper:

- Scalars are denoted by lowercase letters \( x, y, \ldots \).
- Random variables are denoted by uppercase letters \( X, Y, \ldots \).
- Random vectors are denoted by bold lowercase letters \( \mathbf{x}, \mathbf{y}, \ldots \), with \( \text{dim}(\mathbf{x}) \) denoting the dimension of vector \( \mathbf{x} \).
- Finite sets are represented by calligraphic letters \( \mathcal{X}, \mathcal{Y}, \ldots \), with \( \text{dim}(\mathcal{X}) \) denoting the cardinality of set \( \mathcal{X} \).
- Matrices are represented by bold uppercase letters \( \mathbf{A}, \mathbf{B}, \ldots \).
- Matrix operations include trace \( \text{tr}(\cdot) \), determinant \( | \cdot | \), complex-conjugate \( (\cdot)^\ast \), transpose \( (\cdot)^T \), and conjugate transpose \( (\cdot)^H \).
- \( \mathcal{CN}(\mu, \mathbf{K}) \) denotes a circularly symmetric complex-valued Gaussian random vector with mean vector \( \mu \) and covariance matrix \( \mathbf{K} \).
- \( \mathbf{I}_m \) represents the identity matrix of size \( m \).
- Expectation of a random variable is denoted by \( \mathbb{E}\{\cdot\} \).
- The real and imaginary parts of a complex number are denoted as \( \Re\{\cdot\} \) and \( \Im\{\cdot\} \), respectively.

II. PRELIMINARIES

A. MIMO WTC and Improper Signals

A well-known model of physical layer security is WTC, in which a transmitter (Alice) wishes to communicate with a legitimate receiver (Bob) in the presence of an eavesdropper (Eve), as shown in Fig. 1. Denote the number of antennas for Alice, Bob and Eve by \( n_t, n_r, \) and \( n_e \) respectively. Let \( \mathbf{H}_t \in \mathbb{C}^{n_t \times n_r} \) and \( \mathbf{H}_e \in \mathbb{C}^{n_e \times n_r} \) be the channel matrices for the legitimate user and eavesdropper. Then the signals received at Bob and Eve can be formulated as

\[
\begin{align*}
\mathbf{y}_r &= \mathbf{H}_r \mathbf{x} + \mathbf{n}_r, \quad (1a) \\
\mathbf{y}_e &= \mathbf{H}_e \mathbf{x} + \mathbf{n}_e, \quad (1b)
\end{align*}
\]

where \( \mathbf{n}_r \in \mathbb{C}^{n_r \times 1} \) and \( \mathbf{n}_e \in \mathbb{C}^{n_e \times 1} \) are independent proper Gaussian white noise, i.e. \( \mathbf{n}_r \sim \mathcal{CN}(0, \mathbf{I}_{n_r}) \) and \( \mathbf{n}_e \sim \mathcal{CN}(0, \mathbf{I}_{n_e}) \). For the zero-mean complex random vector \( \mathbf{x} \), its covariance matrix and pseudo-covariance matrix are denoted by

\[
\mathbf{K}_x = \mathbb{E}\{\mathbf{x}\mathbf{x}^H\}, \quad \hat{\mathbf{K}}_x = \mathbb{E}\{\mathbf{x}\mathbf{x}^T\},
\]

respectively. \( \mathbf{K}_x \) is Hermitian and positive semidefinite, while \( \hat{\mathbf{K}}_x \) is symmetric. A zero-mean complex random vector \( \mathbf{x} \) is classified as a proper Gaussian signal when the pseudo-covariance matrix \( \mathbf{K}_x \) equals zero; otherwise, it is referred to as an improper signal. It is important to note that for a Gaussian signal, the proper signal corresponds to a symmetric signal, while the improper signal corresponds to an asymmetric signal. Besides, for a pair of Hermitian and positive semidefinite matrix \( \mathbf{K} \) and symmetric matrix \( \hat{\mathbf{K}}_x \), there exists a random vector with covariance and pseudo-covariance given by \( \mathbf{K} \) and \( \hat{\mathbf{K}}_x \) if and only if (iff) the augmented covariance matrix \( \mathbf{K} \) satisfies

\[
\mathbf{K} \begin{bmatrix} \mathbf{K} & \hat{\mathbf{K}}_x \\ \hat{\mathbf{K}}_x^* & \mathbf{K}^* \end{bmatrix} \succeq 0,
\]

i.e., \( \mathbf{K} \) is positive semidefinite [20, Section 2.2.2].

For an arbitrary complex random vector \( \mathbf{x} \) (can be proper or improper) with augmented covariance matrix defined as (2), its differential entropy is

\[
h(\mathbf{x}) = \frac{1}{2} \log[(\pi e)^{2\alpha} |\mathbf{K}_x|].
\]

While for a proper complex random vector \( \mathbf{x} \), its differential entropy is

\[
h(\mathbf{x}) = \log[(\pi e)^{\alpha} |\mathbf{K}_x|].
\]

B. The Secrecy Capacity of Real WTCs

The term secrecy capacity, which was originally described as the maximum rate of reliable transmission, was first introduced by Wyner, as shown in the following definition.
Definition 1 Secrecy Capacity: The concept of perfect secrecy capacity, denoted as \( C_s \), refers to the maximum attainable rate \( R_s \), which ensures the decoding error at the intended receiver and the information leakage at the eavesdropper both converge to zero [2].

A single letter expression of the secrecy capacity of the discrete memoryless (DM) WTC with transition probability \( p(y_r, y_e|x) \) is given in [43] as
\[
C_s = \max_{p(u|x)} \{ I(U; Y_r) - I(U; Y_e) \},
\]
in which the auxiliary random variable \( U \) and signal variables \( X, Y_r \) and \( Y_e \) form a Markov chain \( U \to X \to (Y_r, Y_e) \), where \( |U| \leq |X| \). As for the MIMO real WTC under a sum power constraint [6], it has been proved that the secrecy capacity is
\[
C_s = \max_{K_X \in \kappa} R_s(K_X)
= \max_{K_X \in \kappa} \left\{ \frac{1}{2} \log |I_{2n_r} + H_r K_X H_r^H| \right. \\
\left. \quad - \frac{1}{2} \log |I_{2n_e} + H_e K_X H_e^H| \right\},
\]
where \( \kappa = \{ K_X | K_X \succeq 0, \text{tr}(K_X) \leq P \} \) is the set of all possible covariance matrices and \( R_s(K_X) \) is the maximum achievable secrecy rate between Alice and Bob when the covariance matrix of the transmitted signal is \( K_X \). Here the covariance matrix is defined as \( K_X = E(xx^H) \).

III. THE SECRECY CAPACITY OF THE COMPLEX WTC

Subsequently, we will shift our focus to the case where Wiretap Channels (WTCs) are complex. It is worth noting that any complex system can be equivalently transformed into a real system, allowing us to leverage the equivalent real WTC to determine the secrecy rate of the complex WTC. Notably, we will observe that the secrecy capacity obtained from [6] differs from the results presented in [4] and [5]. The underlying reason behind this disparity will be elucidated in this section, providing valuable insights into the intricacies of the problem.

Theorem 1: The secrecy capacity of the complex MIMO WTC is
\[
C_g = \max_{K_X \in \kappa_g} \left\{ \frac{1}{2} \log |I_{2n_r} + H_r K_X H_r^H| \right. \\
\left. \quad - \frac{1}{2} \log |I_{2n_e} + H_e K_X H_e^H| \right\},
\]
The augmented covariance \( K_X \) is defined in (2) and the augmented channel matrices \( H_r \) and \( H_e \) are defined as
\[
H_r = \begin{bmatrix} H_r & 0 \\ 0 & H^*_e \end{bmatrix}, \quad H_e = \begin{bmatrix} H_e & 0 \\ 0 & H^*_r \end{bmatrix}.
\]
(8)
The feasible set \( \kappa_g = \{ K_X | K_X \succeq 0, \text{tr}(K_X) \leq 2P \} \) is the set of all possible augmented covariance matrices.

Proof: Please refer to Appendix A.

In Theorem 1, the secrecy capacity of complex wiretap channels is expressed with augmented covariance matrix, which is different from the result in [4] and [5], where the secrecy capacity is expressed with only covariance matrix:
\[
C_p = \max_{K_X \in \kappa} R_p(K_X)
= \max_{K_X \in \kappa} \left\{ \log |I_{n_r} + H_r K_X H_r^H| \right. \\
\left. \quad - \log |I_{n_e} + H_e K_X H_e^H| \right\},
\]
(9)
where \( \kappa = \{ K_X | K_X \succeq 0, \text{tr}(K_X) \leq P \} \) is the set of all possible covariance matrices and \( R_p(K_X) \) is the achievable secrecy rate between Alice and Bob when the covariance matrix of the transmitted signal is \( K_X \). [4], [5].

Note that when the transmitted signals are proper, indicated by \( K_X = 0 \), we define the set of augmented covariance matrices for proper signals as \( \kappa_p \), given by
\[
\kappa_p = \{ K_X | K_X = \begin{bmatrix} K_X & 0 \\ 0 & K^*_X \end{bmatrix} \succeq 0, \text{tr}(K_X) \leq 2P \},
\]
(10)
and the corresponding secrecy capacity is given by
\[
C_g = \max_{K_X \in \kappa_g} \left\{ \frac{1}{2} \log |I_{2n_r} + H_r K_X H_r^H| \right. \\
\left. \quad - \frac{1}{2} \log |I_{2n_e} + H_e K_X H_e^H| \right\},
\]
\[
= \max_{K_X \in \kappa_p} \left\{ \frac{1}{2} \log |I_{2n_r} + H_r K_X H_e^H| \right. \\
\left. \quad - \frac{1}{2} \log |I_{2n_e} + H_e K_X H_r^H| \right\}
\]
(11)
which implies that (7) is equivalent to (9) when the transmitted signal is proper, i.e., \( K_X = 0 \). However, if the transmitted signal can be improper, meaning that \( K_X \neq 0 \) is possible, then (7) will differ from (9). In fact, since \( \kappa_p \subseteq \kappa_g \), we always have
\[
C_p \leq C_g
\]
always holds. Although proper Gaussian signals are capacity achieving in many channels, improper Gaussian signals achieve larger rate regions in interference channels when the difference of logarithm-determinant functions appears in the expression of achievable rate. In [4] and [5], the optimality of the proper signal is implicitly assumed without the explanation. Therefore, a Fischer-like determinant inequality is proposed in attempt to prove the optimality of the proper Gaussian signal in the complex degraded WTC in the next section. As a result, the secrecy capacity in (9) is also the secrecy capacity of WTC with general complex signals.

IV. OPTIMALITY OF PROPER SIGNAL FOR THE DEGRADED MIMO WTC

We begin by considering a special case of the WTC known as the degraded WTC. When the channel is degraded, i.e.,
\(H_r^H H_r - H_e^H H_e > 0\) [4, Section 1.C], we define
\[
\Delta = H_r^H H_r - H_e^H H_e > 0,
\]
and let
\[
\Delta = H_r^H H_r - H_e^H H_e = \begin{bmatrix} \Delta & 0 \\ 0 & \Delta^* \end{bmatrix}.
\]
Both \(\Delta\) and \(\Delta\) are positive definite, which means that there exist matrices \(\Delta\) and \(\Delta^*\). To demonstrate the optimality of proper signals in degraded WTCs, we first present several matrix equalities that will be employed in our analysis.

- For any \(A \in C^{n \times n}\) and \(B \in C^{n \times m}\), we have
\[
|lm + AB| = |ln + BA|. \tag{15}
\]
- For any \(A \in C^{n \times n}\), \(B \in C^{n \times n}\) and \(C \in C^{n \times n}\), we have
\[
\begin{bmatrix} A \\ B \end{bmatrix} \begin{bmatrix} A^H & B^H \end{bmatrix} = \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix} \begin{bmatrix} C & C \end{bmatrix} \begin{bmatrix} A^H & 0 \\ 0 & B^H \end{bmatrix}. \tag{16}
\]
- Since elementary row operation and column operation do not change the determinant of a matrix, for a block matrix
\[
A = \begin{bmatrix} A_{11} & A_{12} & A_{13} & A_{14} \\ A_{21} & A_{22} & A_{23} & A_{24} \\ A_{31} & A_{32} & A_{33} & A_{34} \\ A_{41} & A_{42} & A_{43} & A_{44} \end{bmatrix}, \tag{17}
\]
we can interchange the second row with the third row and interchange the second column with the third column at the same time and won’t change the value of the determinant, thus we can obtain
\[
|A| = \begin{bmatrix} A_{11} & A_{13} & A_{12} & A_{14} \\ A_{31} & A_{33} & A_{32} & A_{34} \\ A_{21} & A_{23} & A_{22} & A_{24} \\ A_{41} & A_{43} & A_{42} & A_{44} \end{bmatrix}. \tag{18}
\]

In addition to the aforementioned matrix equalities, we introduce a determinant inequality, similar to Fischer’s determinant inequality, which will play a crucial role in our proof. Consider a square matrix \(A\) of size \(n\), and let \(S_1\) and \(S_2\) be two index sets from the set \([1, 2, \ldots, n]\). We denote \(A(S_1, S_2)\) as the submatrix of \(A\) containing entries that correspond to the rows indexed by \(S_1\) and the columns indexed by \(S_2\). In the case where \(S_1 = S_2\), we refer to \(A(S_1)\) as a principal submatrix of \(A\).

\textbf{Lemma 1:} Let \(K\) be a positive definite \(k \times k\) matrix. Index sets \(S_1, S_2, S_3\) and \(S_4\), which have the form of \(S_1 = [1 : k_1], S_2 = [k_1 + 1 : k_2], S_3 = [k_2 + 1 : k_3]\) and \(S_4 = [k_3 + 1 : k]\), constitute a sequential partition of \([1, 2, \ldots, k]\). Then we have
\[
\frac{|K|}{|K(S_2 \cup S_4)|} \leq \frac{|K(S_1 \cup S_2)|}{|K(S_1)|} \cdot \frac{|K(S_3 \cup S_4)|}{|K(S_3)|}, \tag{19}
\]
with equality if \(K(S_1, S_2, S_3, S_4) = K(S_1 \cup S_3, S_1 \cup S_2) = 0\).

\textbf{Proof:} Please refer to Appendix B.

To provide a clearer illustration of Lemma 1 and its relationship with Fischer’s inequality, we present an example.

\textbf{Example 1:} Consider a Hermitian matrix \(A\) of size \(k \times k\) and a symmetric matrix \(B\) of the same size. We construct the matrix \(K\) as follows:
\[
K = \begin{bmatrix} I + A & A & B & B \\ A & I + A & B & B \\ B^* & B^* & I + A^* & A^* \\ B^* & B^* & A^* & I + A^* \end{bmatrix}. \tag{20}
\]
We choose the index sets as \(S_1 = [1 : k], S_2 = [k + 1 : 2k], S_3 = [2k + 1 : 3k],\) and \(S_4 = [3k + 1 : 4k]\). Applying Lemma 1, we obtain:
\[
\begin{vmatrix} I + A & A \\ A & I + A \end{vmatrix} \leq \begin{vmatrix} I + A & A \\ A & I + A \end{vmatrix} \cdot \begin{vmatrix} I + A^* & A^* \\ A^* & I + A^* \end{vmatrix} \cdot \begin{vmatrix} I + A & 0 \\ 0 & I + A \end{vmatrix}.
\]

By applying Fischer’s inequality, we can deduce that the numerator on the left side of (21) is no greater than the numerator on the right side:
\[
\begin{vmatrix} I + A & A \\ A & I + A \end{vmatrix} \leq \begin{vmatrix} I + A & A \\ A & I + A \end{vmatrix} \cdot \begin{vmatrix} I + A^* & A^* \\ A^* & I + A^* \end{vmatrix} \cdot \begin{vmatrix} I + A & 0 \\ 0 & I + A \end{vmatrix}.
\]

Similarly, the denominator on the left side of (21) is no greater than the denominator on the right side:
\[
\begin{vmatrix} I + A & A \\ A & I + A \end{vmatrix} \leq \begin{vmatrix} I + A & A \\ A & I + A \end{vmatrix} \cdot \begin{vmatrix} I + A^* & A^* \\ A^* & I + A^* \end{vmatrix} \cdot \begin{vmatrix} I + A & 0 \\ 0 & I + A \end{vmatrix}.
\]

Since (22) involves the division of (22) by (23), it is not possible to deduce the inequality relationship in (21) based solely on (22) and (23). However, it is worth noting that the inequality presented in Lemma 1 bears a resemblance to Fischer’s inequality in a fraction form. For a more comprehensive understanding of the connection between Lemma 1 and Fischer’s inequality, please refer to Appendix B.

\textbf{Theorem 2:} The secrecy capacity of degraded complex WTC is achieved when the signal is proper.

\textbf{Proof:} Please refer to Appendix C.
We have proven that proper signals are capacity achieving in degraded complex MIMO WTCs, while improper signals are strictly suboptimal. This important result will serve as the foundation for establishing the optimality of proper signals in the general WTC, as we will demonstrate in the next section. To facilitate our subsequent analysis, we present a modified version of Theorem 2 as the following remark:

Remark 1: From the perspective of optimization, we have

\[
\begin{align*}
\max_{K_x \in \mathcal{K}_p} & \left[ \frac{1}{2} \log |I_{2n_r} + (\Delta + H^H H_x)K_x| - \frac{1}{2} \log |I_{2n_r} + H^H H_x| \right] \\
= & \max_{K_x \in \mathcal{K}_p} \left[ \frac{1}{2} \log |I_{2n_r} + (\Delta + H^H H_x)K_x| - \frac{1}{2} \log |I_{2n_r} + H^H H_x| \right],
\end{align*}
\]

which is more than just the equal optimal value of these two optimization problems with the same objective function and different feasible set. In fact, we have proven that the optimal \( K_x \) can be found in the subset \( \mathcal{K}_p \). Please note that we prove the lemma assuming positive definiteness of both \( \Delta \) and \( \Delta_x \), as we set \( \Delta = H^H \). However, it is worth mentioning that \( \Delta \) and \( \Delta_x \) can also be positive semidefinite.

V. OPTIMALITY OF THE PROPER SIGNAL FOR THE GENERAL COMPLEX MIMO WTC

In this section, we leverage the min-max equivalent reformulation of the secrecy capacity [4], [5]. In the study of WTCs, the min-max reformulation serves as a fundamental tool. Without it, many results related to WTCs would not have been obtained. For instance, when deriving the optimization form of secrecy capacity for WTCs, previous works such as [4], [5], and [6] have all utilized the min-max reformulation. Moreover, most globally optimal algorithms designed for solving the secrecy capacity problem also rely on the min-max reformulation [14], [15], [16]. Even when using the MMSE method, which offers a closed-form solution to the optimization problem, the approach is still based on the min-max reformulation [44]. Therefore, the min-max reformulation is a commonly employed technique in the study of WTCs. By employing these techniques, we can exploit the insights gained from the analysis of the degraded WTC in the previous section to establish the optimality of proper signals for the general MIMO WTC.

Lemma 2: The secrecy capacity of a general MIMO WTC can be equivalently expressed in the form of a min-max optimization problem as

\[
C_g = \min_{\mathbf{A}, K_x \in \mathcal{K}} f_g(Q, K_x) = \max_{\mathbf{A}, K_x \in \mathcal{K}} \left[ \frac{1}{2} \log |I_{2n_r} + n_r^H n_r| - \frac{1}{2} \log |I_{2n_r} + H^H H_x| \right],
\]

where \( H = [H^H, H_x]^T \) and the feasible set \( Q \) are defined as

\[
Q = \{ Q | Q = [I_{2n_r}, A^H I_{2n_r}] > 0 \},
\]

Each feasible matrix \( Q \) in \( Q \) is actually the covariance matrix defined as

\[
Q = E \left\{ \begin{bmatrix} n_r & n_r^T \\ n_r^T & n_r^T \\ n_r^T & n_r^T \\ n_r^T & n_r^T \end{bmatrix} \right\},
\]

so \( A \) is the correlation between augmented noises \( n_r = [n_r^T, n_r^T] \) and \( n_r = [n_r^T, n_r^T] \) as

\[
A = E(n_r n_r^T)
\]

\[
= \left[ \begin{array}{cc} E(n_r n_r^T) & E(n_r n_r^T) \\ E(n_r n_r^T) & E(n_r n_r^T) \end{array} \right] = \left[ \begin{array}{cc} A & E(n_r n_r^T) \\ E(n_r n_r^T) & A^T \end{array} \right].
\]

Proof: The sketch of the proof is in Appendix D. □

We employ the UDL factorization method, as introduced in [4, equation (55)], to decompose \( Q \) as follows:

\[
\begin{bmatrix} I_{2n_r} & A \\ A^H & I_{2n_r} \end{bmatrix}^{-1} = \begin{bmatrix} I_{2n_r} & 0 \\ 0 & I_{2n_r} \end{bmatrix} \begin{bmatrix} I_{2n_r} & A \\ A^H & I_{2n_r} \end{bmatrix} = \begin{bmatrix} I_{2n_r} & 0 \\ 0 & I_{2n_r} \end{bmatrix} \begin{bmatrix} I_{2n_r} & A \\ 0 & I_{2n_r} \end{bmatrix},
\]

so that

\[
\begin{bmatrix} I_{2n_r} & A \\ A^H & I_{2n_r} \end{bmatrix}^{-1} = \begin{bmatrix} I_{2n_r} & 0 \\ 0 & I_{2n_r} \end{bmatrix} \begin{bmatrix} I_{2n_r} & A \\ A^H & I_{2n_r} \end{bmatrix}^{-1} \begin{bmatrix} I_{2n_r} & 0 \\ 0 & I_{2n_r} \end{bmatrix} \begin{bmatrix} I_{2n_r} & A \\ 0 & I_{2n_r} \end{bmatrix},
\]

from which we obtain

\[
H^H Q^{-1} H = (H^H - H^H A^H) (I_{2n_r} - A A^H)^{-1} (H^H - A H). \]

Thus, we can rewrite the secrecy capacity \( C_g \) as (32)

\[
C_g = \min_{\mathbf{A}, K_x \in \mathcal{K}} \max_{\mathbf{A}, K_x \in \mathcal{K}} \left[ \frac{1}{2} \log |I_{2n_r} + n_r^H n_r| - \frac{1}{2} \log |I_{2n_r} + H^H H_x| \right],
\]

where the feasible set \( \mathcal{A} \) is defined as

\[
\mathcal{A} = \{ A | I_{2n_r} - A A^H > 0 \}.
\]

Given that the objective function in (32) is convex with respect to \( A \) and concave with respect to \( K_x \), we can establish that the min-max problem is equivalent to the max-min problem, and the optimal solution corresponds to a saddle point [4, Proposition 5].

If the feasible set \( \mathcal{A} \) is contracted to a smaller set \( \mathcal{A}' \) as

\[
\mathcal{A}' = \left\{ A | A = [A, 0^T] \right\} \begin{bmatrix} I_{2n_r} & 0 \\ 0 & A^T \end{bmatrix} \begin{bmatrix} I_{2n_r} & 0 \\ 0 & A^T \end{bmatrix} > 0 \},
\]
then the minimization in the set $A'$ will yield an upper bound of $C_g$. Denote the optimal $K_x$ by $K_x^*$, then we have

$$C_g = \max_{K_x \in \mathcal{K}} \min_{A \in \mathcal{A}} C_g(A, K_x) = \min_{A \in \mathcal{A}} C_g(A, K_x^*) \leq \min_{A \in \mathcal{A}'} C_g(A, K_x^*) \leq \max_{K_x \in \mathcal{K}} \min_{A \in \mathcal{A}'} C_g(A, K_x)$$

where (a) follows since contracting the feasible set $A$ to $A'$ may lead to a new optimal $K_x$ rather than $K_x^*$. Set $\hat{A}$ is still a convex set, so the max-min is equal to min-max. It means

$$C_g \leq \min_{A \in \hat{A}} \max_{K_x \in \mathcal{K}} C_g(A, K_x).$$

As each of the $A \in \hat{A}$ is a block diagonal matrix, according to (37), as shown at the bottom of the next page, $(H^H - H_e^H A^H)(I - A A^H)^{-1}(H_e - A H_e)$ is also a block diagonal matrix. In addition, it is positive semi-definite, since $H^H Q^{-1} H$ can be easily proved to be positive semi-definite. Hence we can denote it by $\Delta$ with the form of

$$\Delta = \begin{bmatrix} \Delta & 0 \\ 0 & \Delta^\perp \end{bmatrix}.$$ (38)

where $\Delta$ and $\Delta^\perp$ are both positive semi-definite with the existence of $\Delta_+^2$ and $\Delta_-^2$. Now we can use the result of the degraded WTCs and get the following theorem.

Theorem 3: The secrecy capacity of general complex WTC is achieved when the signal is proper.

Proof: Please refer to Appendix E.

Consequently, we can conclude that proper signals not only achieve the capacity in degraded complex MIMO WTCs, but they are also capacity-achieving in general complex MIMO WTCs. On the other hand, it is evident that improper signals are strictly sub-optimal since equality in (75) holds only when the signals are proper. This signifies the significance of employing proper signals in achieving the maximum secrecy rate in general complex MIMO WTCs.

Remark 2: We only consider WTCs with full channel state information (CSI) of the legitimate user and eavesdropper. In this remark, we assume that only statistical CSI of the eavesdropper is available at the transmitter. Then the secrecy capacity $C_p$ of the MISO WTC with proper transmitted signals is [45]

$$C_p = \max_{\|K_x\|_{\mathcal{K}} \leq P} \left[ \frac{1}{2} \log |I_2 + H_e K_x H_e^H| - \frac{1}{2} \log |I_2 + H_x K_x H_e^H| \right],$$

where $h_e$ and $h_x$ are row vectors. The statistical distribution of $h_e$ is known at the transmitter. Additionally, we investigate the secrecy capacity when general transmitted signals are used, denoted as $C_g$. Its expression is given by:

$$C_g = \max_{\|K_x\|_{\mathcal{K}} \leq P} \left[ \frac{1}{2} \log |I_2 + H_e K_x H_e^H| - \frac{1}{2} \mathbb{E}_{h_x} \{ \log |I_2 + H_x K_x H_e^H| \} \right].$$ (40)

where

$$H_e = \begin{bmatrix} h_e & 0 \\ 0 & h_e' \end{bmatrix}, \quad H_x = \begin{bmatrix} h_x & 0 \\ 0 & h_x' \end{bmatrix}.$$ (41)

Intuitively, we hypothesize that proper signals remain optimal even in MISO WTC scenarios with statistical CSI. To illustrate this concept, we provide a simplified example using a specific channel matrix for the legitimate user $h_x$ and the probability distribution of the eavesdropper’s channel matrix $h_e$.

$$h_e = \begin{bmatrix} 2.461 + 4.719i, 0.867 - 4.458i, -1.052 + 3.278i \end{bmatrix}.$$ (42)

The distribution of the channel matrix for the eavesdropper is

$$\Pr(h_e = h_{e_1}) = 1/6,$$

$$\Pr(h_e = h_{e_2}) = 1/3,$$

$$\Pr(h_e = h_{e_3}) = 1/2,$$ (43)

Then the secrecy rates curves using ADCF algorithm is depicted as follows. We can see two curves converge to the same value, which means the proper signals are also optimal. This is intuitively correct for we can rewrite the secrecy capacity for this channel as

$$C_g = \max_{\|K_x\|_{\mathcal{K}} \leq P} \left[ \frac{1}{2} \log |I_2 + H_e K_x H_e^H| - \frac{1}{2} \log |I_2 + H_x K_x H_e^H| \right],$$

$$\Pr(h_e = h_{e_1}) = 1/6,$$

$$\Pr(h_e = h_{e_2}) = 1/3,$$

$$\Pr(h_e = h_{e_3}) = 1/2,$$ (44)

This assertion is grounded in the fact that we can express the secrecy capacity for this channel in a way that resembles a mixture of optimal signals for three virtual wiretap channels, each corresponding to a particular eavesdropper’s channel matrix. As these individual channels have proper signals as their optima, it follows that the combined channel also exhibits proper signaling as an optimal strategy.

VI. NUMERICAL RESULTS

In order to compare the maximum achievable rates of proper signals and general complex signals in complex MIMO WTCs under the sum power constraint $P$, we conduct numerical experiments to validate our theoretical findings. As we have previously established that proper signals are capacity-achieving in WTCs, problem (7) is equivalent to (9).
ADCA and PBRA algorithms for WTCs and present numerical signals, which is impractical. Hence, we utilize the efficient require an exhaustive examination of all possible improper signals. Conversely, proving the optimality of proper signals would be difficult.

To establish the superiority of improper signals, it is sufficient to design a separate matrix corresponds to an improper signal, while the zero covariance and pseudo-covariance optimization algorithm, it is not feasible to prove the optimality of proper signals using this case are -9.5854, 27.0768, and 62.6697. We assume that the noises are proper Gaussian with zero mean vectors and identical covariance matrices \( I \) has at least one positive eigenvalue to guarantee positive secrecy capacity [46]. The eigenvalues for this case are -9.5854, 27.0768, and 62.6697. We assume that the noises are proper Gaussian with zero mean vectors and identical covariance matrices \( I \), resulting in a signal-to-noise ratio (SNR) of SNR = 10 log \( \left( \frac{P}{n} \right) \).

For our numerical analysis, we employ the ADCA and PBRA algorithms, which were designed and evaluated in [16]. It is important to note that the focus of our work is not algorithm design or improvement. While [34] demonstrates the superiority of improper signals by designing a separate covariance and pseudo-covariance optimization algorithm, it is not feasible to prove the optimality of proper signals using numerical algorithms. This is due to the fact that, given a fixed covariance matrix, each non-zero pseudo-covariance matrix corresponds to an improper signal, while the zero pseudo-covariance matrix corresponds to the proper signal. To establish the superiority of improper signals, it is sufficient to find a single improper signal that outperforms the proper signal in a specific channel through numerical experiments. Conversely, proving the optimality of proper signals would require an exhaustive examination of all possible improper signals, which is impractical. Hence, we utilize the efficient ADCA and PBRA algorithms for WTCs and present numerical results that compare the secrecy capacity achieved by general complex signals and proper signals.

The ADCA algorithm leverages the difference-of-convex optimization form of the objective function. As we know, maximizing a logarithmic determinant function is a convex optimization problem. In (7) and (9), the objective function is the difference between two logarithm functions, allowing us to linearize the logarithmic determinant function after the subtraction. This leads to a strictly suboptimal convex optimization problem. Through iterations, the optimal values of a series of suboptimal convex optimization problems converge to the local optimal value of the original optimization problem. On the other hand, PBRA employs the min-max reformulation given by (25) and (71). Let us consider (25) as an illustrative example, although the same steps apply to (71). To solve (7), we can solve (25) by initializing with an arbitrary \( \mathbf{Q}_t \) and obtaining the optimal \( \mathbf{k}_x \). With \( \mathbf{k}_x \), we can calculate another optimal \( \mathbf{Q}_2 \). By iteratively solving for the optimal \( \mathbf{k}_x \) and \( \mathbf{Q}_t \), PBRA converges to the saddle point of (25).

### A. Convergence Results

Figures 3 and 4 illustrate the convergence rates for SNR = 10 dB and SNR = 15 dB, respectively.

In both figures, we observe four convergence rate curves. The solid curve with square markers represents the convergence rate for the general complex signal solved using ADCA, corresponding to problem (7) with ADCA. The dashed curve with plus markers represents the convergence rate for the proper signal solved using ADCA, corresponding to problem (9) with ADCA. The solid curve with circle markers represents the convergence rate for the general complex signal solved using PBRA, corresponding to problem (7) with PBRA. Finally, the dashed curve with cross markers represents the convergence rate for the proper signal solved using PBRA,

$$
\begin{align*}
\mathbf{H}_r &= \begin{bmatrix}
-1.468 - 3.110i & -3.310 + 1.256i & -0.491 + 2.757i \\
3.212 + 1.868i & 1.491 + 2.802i & 0.470 - 0.132i \\
-4.846 - 3.165i & 2.317 - 4.189i & -2.037 - 0.641i
\end{bmatrix}, \\
\mathbf{H}_e &= \begin{bmatrix}
-1.937 - 1.493i & 3.176 + 0.502i & -1.214 - 2.923i \\
0.085 + 4.390i & 2.948 + 1.225i & 3.116 - 1.988i \\
0.108 + 3.759i & 1.443 + 0.870i & 0.328 - 0.291i
\end{bmatrix}.
\end{align*}
$$

These channel matrices are generated randomly while ensuring that \( \mathbf{H}_r^H \mathbf{H}_r - \mathbf{H}_e^H \mathbf{H}_e \) has at least one positive eigenvalue to guarantee positive secrecy capacity [46]. The eigenvalues for this case are -9.5854, 27.0768, and 62.6697. We assume that the noises are proper Gaussian with zero mean vectors and identical covariance matrices \( I \), resulting in a signal-to-noise ratio (SNR) of SNR = 10 log \( \left( \frac{P}{n} \right) \).

For our numerical analysis, we employ the ADCA and PBRA algorithms, which were designed and evaluated in [16]. It is important to note that the focus of our work is not algorithm design or improvement. While [34] demonstrates the superiority of improper signals by designing a separate covariance and pseudo-covariance optimization algorithm, it is not feasible to prove the optimality of proper signals using numerical algorithms. This is due to the fact that, given a fixed covariance matrix, each non-zero pseudo-covariance matrix corresponds to an improper signal, while the zero pseudo-covariance matrix corresponds to the proper signal. To establish the superiority of improper signals, it is sufficient to find a single improper signal that outperforms the proper signal in a specific channel through numerical experiments. Conversely, proving the optimality of proper signals would require an exhaustive examination of all possible improper signals, which is impractical. Hence, we utilize the efficient ADCA and PBRA algorithms for WTCs and present numerical results that compare the secrecy capacity achieved by general complex signals and proper signals.

The ADCA algorithm leverages the difference-of-convex optimization form of the objective function. As we know, maximizing a logarithmic determinant function is a convex optimization problem. In (7) and (9), the objective function is the difference between two logarithm functions, allowing us to linearize the logarithmic determinant function after the subtraction. This leads to a strictly suboptimal convex optimization problem. Through iterations, the optimal values of a series of suboptimal convex optimization problems converge to the local optimal value of the original optimization problem. On the other hand, PBRA employs the min-max reformulation given by (25) and (71). Let us consider (25) as an illustrative example, although the same steps apply to (71). To solve (7), we can solve (25) by initializing with an arbitrary \( \mathbf{Q}_t \) and obtaining the optimal \( \mathbf{k}_x \). With \( \mathbf{k}_x \), we can calculate another optimal \( \mathbf{Q}_2 \). By iteratively solving for the optimal \( \mathbf{k}_x \) and \( \mathbf{Q}_t \), PBRA converges to the saddle point of (25).

$$
\begin{align*}
\mathbf{H}_r^H - \mathbf{H}_e^H \mathbf{A}^H (\mathbf{I} - \mathbf{A} \mathbf{A}^H)^{-1} (\mathbf{H}_r - \mathbf{A} \mathbf{H}_e) \\
= \begin{bmatrix}
(\mathbf{H}_r^H - \mathbf{H}_e^H \mathbf{A}^H) (\mathbf{I}_{n_R} - \mathbf{A} \mathbf{A}^H)^{-1} (\mathbf{H}_r - \mathbf{A} \mathbf{H}_e) \\
0
\end{bmatrix} \\
= \mathbf{A}
\end{align*}
$$

(A)
corresponding to problem (9) with PBRA. Notably, all four curves converge to nearly the same value after iteration, as evident in both figures.

When solving problems (7) and (9) with ADCA, we initialize the algorithm with $K_x = I_6$ for the general complex signal case and $K_x = I_3$ for the proper signal case. Similarly, when using PBRA to solve problems (7) and (9), we employ the same initial point $Q = I_{14}$ for the general complex signal case and $Q = I_7$ for the proper signal case. We terminate the iterations when the change between two consecutive iterative points falls below $10^{-5}$.

Interestingly, we find that the two ADCA convergence curves, one for the general complex signal and the other for the proper signal, are identical. This is because they actually start from the same initial point. A general complex signal with an augmented covariance matrix $K_x = I_6$ is equivalent to a proper signal with a covariance matrix $K_x = I_3$. A similar analysis applies to the PBRA convergence curves for general complex signals and proper signals. However, this does not compromise the generality of our numerical results. Since it has been proven in [47] that problems (7) and (9) have unique solutions, the choice of initial points does not impact the resulting values in any of the four cases. This observation also explains why ADCA and PBRA return the same value, despite ADCA being a local optimizer and PBRA being a global optimizer.

### B. Secrecy Rates for More Channel Realizations

We present additional secrecy rate results, computed using both PBRA and ADCA algorithms, for various channel scenarios. Specifically, Channel 1 is defined in (46), while Channels 2 through 4 are characterized by the expressions given in (47) to (49), as shown at the bottom of the next page.

$$H_r = \begin{bmatrix} -2.057 & -2.876i & 0.811 - 0.555i & -4.440 + 2.962i \\ -3.201 + 0.433i & 1.372 - 4.146i & 3.169 + 1.912i \\ 4.263 + 2.025i & 1.513 - 4.427i & 0.289 - 1.547i \\ -4.318 + 4.564i & 3.646 + 1.295i & 1.944 + 4.468i \end{bmatrix}.$$ \hspace{1cm} (47)

The results are presented in Table I, where we employed both the PBRA and ADCA algorithms to compute the maximum secrecy rates separately for general and proper signals in each channel scenario. Of particular interest to us is the Gap, which quantifies the difference in secrecy rates between general and proper signals. The Gap is calculated as follows:

$$\text{Gap} = |\text{PBRA general} + \text{ADCA general} - \text{PBRA proper} - \text{ADCA proper}|.$$ \hspace{1cm} (50)

Notably, the largest Gap observed in our results is 0.0016, indicating that the secrecy capacity of the wiretap channel is indeed achieved when employing proper signals.

### C. Secrecy Capacity via SNR

In this subsection, we analyze the secrecy capacity achieved by proper signals and general complex signals using ADCA and PBRA across a range of signal-to-noise ratios (SNRs). Figure 5 displays the results for SNRs ranging from 1 dB to 25 dB. Notably, when the SNR is set to 11 dB, we observe that the secrecy capacity values for the four cases exhibit a maximum gap of 0.0016. This finding allows us to confidently
assert that, based on these numerical experiments, proper signals are indeed capacity-achieving in MIMO WTCs.

VII. CONCLUSION

In this study, we have demonstrated the optimality of proper complex signals in the multiple-input multiple-output (MIMO) wiretap channel (WTC). Previous works have assumed the transmitted signal to be proper in the complex WTC without explanations, and we have shown that this assumption is always correct. We have proposed a new determinant function to prove that the secrecy rate of a complex Gaussian signal with a fixed covariance matrix is maximized when the signal is proper in a degraded complex WTC. We have also shown that this result holds for the general complex WTC using a min-max reformulation of the secrecy capacity.

It is important to acknowledge that the approach presented in this study may not be directly applicable to channels with different expressions for the achievable rate. However, our work sheds light on the relationship between the optimality of proper signals and optimization problems. Specifically, when the capacity or achievable rate of a complex channel exhibits convexity or can be reformulated as a convex optimization problem, the use of proper signals tends to yield optimal solutions.

Regarding the application of our findings in real wireless system design, we offer the following insight: In scenarios

where Quadrature Amplitude Modulation (QAM) or Orthogonal Frequency Division Multiplexing (OFDM) schemes are employed for WTCs, our research suggests a valuable approach. Specifically, by setting orthogonal signals independently with equal power levels, practitioners can achieve higher transmission rates. This practical implication stems from our theoretical work, which establishes the optimality of proper signals.

Furthermore, our findings establish a connection between the uniqueness of solutions, as explored in recent works [47], [48], and our investigation. In cases where improper signals are deemed optimal, we can always identify a pair of improper signals. This connection broadens the implications of our study, potentially impacting the broader exploration of complex channels in various contexts.

APPENDIX A

By considering a complex signal $x = R[x] + i3[x] \in \mathbb{C}^{n \times 1}$, we can interpret it as a joint real signal $\hat{x} = (R[x]^T, i3[x]^T)^T \in \mathbb{R}^{2n \times 1}$. Accordingly, the complex MIMO WTC (1) can be equivalently expressed as a real MIMO WTC with input $\hat{x}$:

\begin{equation}
\begin{bmatrix}
\sqrt{2}R(y_r) \\
\sqrt{2}R(y_i)
\end{bmatrix}
= \begin{bmatrix}
\sqrt{2}R(H_r) \\
\sqrt{2}R(H_i)
\end{bmatrix}
\begin{bmatrix}
R[x] \\
i3[x]
\end{bmatrix}
\end{equation}

\begin{equation}
\begin{bmatrix}
\sqrt{2}R(y_e) \\
\sqrt{2}R(y_o)
\end{bmatrix}
= \begin{bmatrix}
\sqrt{2}R(H_e) \\
\sqrt{2}R(H_o)
\end{bmatrix}
\begin{bmatrix}
R[x] \\
i3[x]
\end{bmatrix}
\end{equation}

(51a)

\begin{equation}
\begin{bmatrix}
\sqrt{2}R(y_r) \\
\sqrt{2}R(y_i)
\end{bmatrix}
= \begin{bmatrix}
\sqrt{2}R(H_r) \\
\sqrt{2}R(H_i)
\end{bmatrix}
\begin{bmatrix}
R[x] \\
i3[x]
\end{bmatrix}
\end{equation}

\begin{equation}
\begin{bmatrix}
\sqrt{2}R(y_e) \\
\sqrt{2}R(y_o)
\end{bmatrix}
= \begin{bmatrix}
\sqrt{2}R(H_e) \\
\sqrt{2}R(H_o)
\end{bmatrix}
\begin{bmatrix}
R[x] \\
i3[x]
\end{bmatrix}
\end{equation}

(51b)
where the constant $\sqrt{2}$ is multiplied to scale the noises $\tilde{n}_v$ and $\tilde{n}_r$ with an identity covariance matrix.

We denote the covariance of $\tilde{x}$ by $K_x$, then we have

$$K_x = \mathbb{E} \left[ \begin{bmatrix} R(x) \\ \tilde{G}(x) \end{bmatrix} \begin{bmatrix} R(x) \\ \tilde{G}(x) \end{bmatrix}^T \right].$$  \hfill (52)

According to (6), we can characterize the secrecy capacity of this equivalent real WTC as

$$C_s = \max_{K_x \succeq 0, t \leq 2p} \left[ \frac{1}{2} \log |I_{2r} + \tilde{H} K_x \tilde{H}^T| - \frac{1}{2} \log |I_{2r} + \tilde{H} \tilde{K}_r \tilde{H}^T| \right].$$  \hfill (53)

Notably, information measures such as entropy and mutual information are determined by the probability distribution of the signal, rather than the specific values within the signal space. As a result, the secrecy capacity of the original complex channel is equal to the secrecy capacity of this equivalent real channel (51). Hence, (53) is essentially the desired secrecy capacity for the complex MIMO WTC. However, the elegance of the expression will lose with real matrices from the equivalent real WTC [49]. Therefore, we will rewrite the formula (53) with notations from the original complex MIMO WTC.

It was shown in [20] that the matrices $K_x$ and $K_r$ can be expressed as follows:

$$K_x = \frac{1}{4} M_n^H K_x M_n, \quad K_r = \frac{\sqrt{2}}{2} M_n^H H_n M_n,$$  \hfill (54)

where $M_n$ is a unitary matrix of size $2n_1$ given by:

$$M_n = \begin{bmatrix} I_{n_1} & iI_{n_1} \\ I_{n_1} & -iI_{n_1} \end{bmatrix},$$  \hfill (55)

and it satisfies the relation:

$$M_n M_n^H = M_n^H M_n = 2I_{2n_1}. \hfill (56)$$

By substituting (54) and (56) into (53), we obtain the secrecy capacity of the complex MIMO WTC as:

$$C_s = C_g = \max_{K_x \in K_g} \left[ \frac{1}{2} \log |I_{2r} + \tilde{H} K_x \tilde{H}^T| - \frac{1}{2} \log |I_{2r} + \tilde{H} \tilde{K}_r \tilde{H}^T| \right],$$  \hfill (57)

where $K_g$ represents the result with complex matrices from the complex WTC.

**APPENDIX B**

**A. Proof of Lemma 1**

For any positive semidefinite matrix $K$, we can find a proper random vector $x$ so that $K = \mathbb{E}[x \cdot x^H]$. We can partition $x$ to four sub random vectors $x_i: i = 1, 2, 3, 4$ as

$$x^H = \begin{bmatrix} x_1^H \\ x_2^H \\ x_3^H \\ x_4^H \end{bmatrix},$$  \hfill (58)

where the dimension of $x_i$ coincides with the dimension of $S_i$, i.e. $\dim(x_i) = \dim(S_i)$. $x_i: i = 1, 2, 3, 4$ are all proper complex random vectors as $x$ is proper. According to (4), we have

$$h(x_1, x_2, x_3, x_4) = \log((\pi e)^{K_1}),$$  \hfill (59a)

$$h(x_2, x_4) = \log((\pi e)^{K_2 + K_3}),$$  \hfill (59b)

$$h(x_1, x_2) = \log((\pi e)^{K_4 + K_5}),$$  \hfill (59c)

$$h(x_1, x_4) = \log((\pi e)^{K_6 + K_7}),$$  \hfill (59d)

$$h(x_2) = \log((\pi e)^{K_8}),$$  \hfill (59e)

$$h(x_4) = \log((\pi e)^{K_9}).$$  \hfill (59f)

Now consider the conditional entropy inequality

$$h(x_1, x_3| x_2, x_4) = h(x_1|x_2, x_4) + h(x_3|x_1, x_2, x_4) \leq h(x_1|x_2) + h(x_3|x_4).$$  \hfill (60)

Substituting (59) into (60), we obtain the desired result.

**B. Connection With Fischer’s Inequality**

Now we can reveal the more comprehensive connection with Fischer’s inequality. Assume $A$ and $C$ are positive semidefinite complex matrices of size $p \times p$ and $q \times q$, respectively, while $B$ is a complex matrix of size $p \times q$. Let us define the matrix $M$ as:

$$M = \begin{bmatrix} A & B \\ B^H & C \end{bmatrix}. \hfill (61)$$

In this context, Fischer’s inequality can be stated as follows:

$$|M| \leq |A||C|. \hfill (62)$$

Traditionally, Fischer’s inequality is proven using matrix analysis techniques. However, it can also be established using a basic entropy inequality. For any positive semidefinite matrix $M$, we can find an appropriate random vector $x$ such that $M = \mathbb{E}[x \cdot x^H]$ with a length of $p + q$. Let $x_1$ represent the first $p$ elements of $x$, and $x_2$ denote the last $q$ elements of $x$. We then have:

$$h(x) = h(x_1, x_2) \leq h(x_1) + h(x_2).$$  \hfill (63)

which directly corresponds to Fischer’s inequality, as

$$h(x) = \log((\pi e)^{P + q}|M|),$$  \hfill (64a)

$$h(x_1) = \log((\pi e)^p|A|),$$  \hfill (64b)

$$h(x_2) = \log((\pi e)^q|C|).$$  \hfill (64c)

This alternative approach reveals the equivalence between the entropy inequality and Fischer’s inequality. Moreover, this alternative approach highlights a crucial insight: the inequality derived in Lemma 1 shares a fundamental similarity with Fischer’s inequality. Notably, Fischer’s inequality emerges from the basic entropy inequality, while our inequality arises from the basic conditional inequality.

**APPENDIX C**

Let $x$ denote a general Gaussian complex signal with a covariance matrix $K_x$ and a pseudo-covariance matrix $\tilde{K}_x$. The secrecy rate achieved when transmitting $x$ can be expressed as follows:

$$\frac{1}{2} \log |I_{2n_1} + \tilde{H} \tilde{K}_x \tilde{H}^T| - \frac{1}{2} \log |I_{2n_r} + \tilde{H} \tilde{K}_r \tilde{H}^T|$$
where (a) follows from (16), (b) follows from (15) and (c) follow from (18). Next, denote $K$ as

$$K = I_{2(n_t+n_e)} + \left[ \begin{array}{cccc} \Delta^\frac{1}{2} & 0 & 0 & 0 \\ 0 & \Delta^\frac{1}{2} & 0 & 0 \\ 0 & 0 & \Delta^\frac{1}{2} & 0 \\ 0 & 0 & 0 & \Delta^\frac{1}{2} \end{array} \right] \times \left[ \begin{array}{cccc} K_x & K_x & K_x & K_x \\ K_x & K_x & K_x & K_x \\ K_x & K_x & K_x & K_x \\ K_x & K_x & K_x & K_x \end{array} \right]$$

and divide $K$'s index set $\{1 : 2(n_t+n_e)\}$ into $S_1 = [1 : n_t], S_2 = [n_t + 1 : n_t + n_e], S_3 = [n_t + n_e + 1 : 2n_t + n_e]$ and $S_4 = [2n_t + n_e + 1 : 2(n_t + n_e)]$, then we can express (65) neatly as follows:

$$\frac{1}{2} \log I_{2(n_t+n_e)} + \left[ \begin{array}{cccc} \Delta^\frac{1}{2} & 0 & 0 & 0 \\ 0 & \Delta^\frac{1}{2} & 0 & 0 \\ 0 & 0 & \Delta^\frac{1}{2} & 0 \\ 0 & 0 & 0 & \Delta^\frac{1}{2} \end{array} \right] \times \left[ \begin{array}{cccc} K_x & K_x & K_x & K_x \\ K_x & K_x & K_x & K_x \\ K_x & K_x & K_x & K_x \\ K_x & K_x & K_x & K_x \end{array} \right]$$

where (a) follows from (15), (b) follows from (14), (c) follows from (16) and (d) follows from (18). For any $K_x \in \mathcal{K}$, with equality iff $\tilde{K}_x = 0$. In the proof, (a) follow from (16), (b) follow from (15) and (c) follow from (13). As a result, if $x$ is Gaussian with a given covariance matrix $K_x$, its secrecy rate is maximized if $x$ is proper, from which we get

$$C_x \leq C_p.$$  \hfill (69)

(69) combined with (12) can yield

$$C_x = C_p.$$  \hfill (70)

\section*{Appendix D}

The proof follows a similar approach to that of Theorem 1. Oggier et al. [4] presented the min-max reformulation for (9)
as follows:

\[
C_p = \min_{Q \in \mathcal{Q}, K_e \in \mathcal{K}_e} \max_{K_r \in \mathcal{K}_r} f_p(Q, K_r) = \min_{Q \in \mathcal{Q}, K_e \in \mathcal{K}_e} \left[ \log |I_{n_r + n_e} + Q^{-1}HK_eH^H| - \log |I_{n_e} + H_eK_eH_e^H| \right].
\]

(71)

where \( H = [H_e^T, H_e^T] \) and the feasible set \( \mathcal{Q} \) is defined as

\[
\mathcal{Q} = \{ Q | Q = [A_H A], A > 0 \}.
\]

(72)

which is the covariance matrix defined as

\[
Q = \mathbb{E} \left[ \begin{bmatrix} n_r \mid n_r \end{bmatrix} \begin{bmatrix} n_r^H \mid n_r^H \end{bmatrix} \right],
\]

(73)

so \( A \) is the correlation between noises \( n_r \) and \( n_e \) as \( A = \mathbb{E}[n_r n_e^H] \). Then we can find the corresponding result for real signals. Since we can view the general complex signal as a real signal composed of the real part and imaginary part of the original complex signal, the min-max reformulation for the general complex WTC can be obtained.

**APPENDIX E**

Since \( I_{2n_r} - AA^H > 0 \) is equivalent to \( I_{n_r} - AA^H > 0 \), we define \( A \) as

\[
A = \{ A \mid A^H > 0 \}.
\]

(74)

Then we can prove that \( C_p \) is the upper bound of \( C_g \) as (75)

\[
C_g \leq \min_{A \in \mathcal{A}} \left[ \frac{1}{2} \log |I_{2n_r} + (H_e^H - H_e^H A^H)(I - AA^H)^{-1}(H_e - A H_e) + H_e^H H_e|K_s| \right]
\]

\[
- \frac{1}{2} \log |I_{2n_e} + H_e K_e H_e^H| \right] \right]
\]

\[
= \min_{A \in \mathcal{A}} \left[ \frac{1}{2} \log |I_{2n_r} + (\Delta + H_e^H H_e)|K_s| \right] - \frac{1}{2} \log |I_{2n_e} + H_e K_e H_e^H| \right] \right]
\]

\[
= \min_{A \in \mathcal{A}} \left[ \frac{1}{2} \log |I_{n_r} + (\Delta + H_e^H H_e)|K_s| \right] - \log |I_{n_e} + H_e K_e H_e^H| \right] \right]
\]

\[
= \min_{Q \in \mathcal{Q}, K_e \in \mathcal{K}_e} [Q_{n_r + n_e} + Q^{-1}HK_eH^H]
\]

\[
- \log |I_{n_r} + H_e K_e H_e^H| \right] \right] \right]
\]

\[
= \min_{Q \in \mathcal{Q}, K_e \in \mathcal{K}_e} [Q_{n_r + n_e} + Q^{-1}HK_eH^H]
\]

\[
- \log |I_{n_r} + H_e K_e H_e^H| \right] \right] \right]
\]

\[
(d) \leq C_p,
\]

(75)

where (a) follow from (36), (b) follow from (37), (c) follows since Remark 1 is valid for any \( A \in \mathcal{A} \), so we have shown \( C_g \leq C_p \) holds for WTC, and (d) follow from (71). In addition, \( C_p \leq C_g \) always holds as the proper signal is a special case of the general complex signal, so we have \( C_g = C_p \), which finishes the proof.

**REFERENCES**

[1] C. E. Shannon, “Communication theory of secrecy systems,” Bell Syst. Tech. J., vol. 28, no. 4, pp. 656–715, Oct. 1949.

[2] A. D. Wyner, “The wire-tap channel,” Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[3] S. Leung-Yan-Cheong and M. Hellman, “The Gaussian wire-tap channel,” IEEE Trans. Inf. Theory, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.

[4] F. Oggier and B. Hassibi, “The secrecy capacity of the MIMO wiretap channel,” IEEE Trans. Inf. Theory, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[5] A. Khisti and G. W. Wornell, “Secure transmission with multiple antennas—Part II: The MIMO MISO wiretap channel,” IEEE Trans. Inf. Theory, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[6] T. Liu and S. Shamai (Shitz), “A note on the secrecy capacity of the multiple-antenna wiretap channel,” IEEE Trans. Inf. Theory, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

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

[8] J. Li and A. Petropulu, “Optimal input covariance for achieving secrecy capacity in Gaussian MIMO wiretap channels,” in Proc. IEEE Int. Conf. Acoust., Speech Signal Process., Dallas, TX, USA, Mar. 2010, pp. 3362–3365.

[9] P. L. Cao and T. J. Oechtering, “Optimal transmit strategies for Gaussian MISO wiretap channels,” IEEE Trans. Inf. Forensics Security, vol. 15, pp. 829–838, 2020.

[10] S. Loyka and D. Charalambous, “Optimal signaling for secure communications over Gaussian MIMO wiretap channels,” IEEE Trans. Inf. Theory, vol. 62, no. 12, pp. 7207–7215, Dec. 2016.

[11] S. Ali, A. Fakoorian and A. L. Swindlehurst, “Full rank solutions for the Gaussian MIMO wiretap channel with an average power constraint,” IEEE Trans. Signal Process., vol. 61, no. 10, pp. 2620–2631, May 2013.

[12] K. Cumanan, Z. Ding, B. Sharif, G. Y. Tian, and K. K. Leung, “Secrecy rate optimizations for a MIMO secrecy channel with a multiple-antenna eavesdropper,” IEEE Trans. Veh. Technol., vol. 63, no. 4, pp. 1678–1690, May 2014.

[13] T. V. Nguyen, Q.-D. Vu, M. Juntti, and L.-N. Tran, “A low-complexity algorithm for achieving secrecy capacity in MIMO wiretap channels,” in Proc. IEEE Int. Conf. Comun. (ICC), Dublin, Ireland, Jun. 2020, pp. 1–6.

[14] S. Loyka and D. Charalambous, “An algorithm for global maximization of secrecy rates in Gaussian MIMO wiretap channels,” IEEE Trans. Commun., vol. 63, no. 6, pp. 2288–2299, Jun. 2015.

[15] L. Dong, S. Loyka, and Y. Li, “Algorithms for globally-optimal secure signaling over Gaussian MIMO wiretap channels under interference constraints,” IEEE Trans. Signal Process., vol. 68, pp. 4513–4528, 2020.

[16] A. Mukherjee, B. Ottersten, and L.-N. Tran, “On the secrecy capacity of MIMO wiretap channels: Convex reformulation and efficient numerical methods,” IEEE Trans. Commun., vol. 69, no. 10, pp. 6865–6878, Oct. 2021.

[17] H. Xu, G. Caire, and C. Pan, “An achievable region for the multiple access wiretap channels with confidential and open messages,” in Proc. IEEE Int. Symp. Inf. Theory (ISIT), Jun. 2020, pp. 949–954.

[18] H. Xu, K.-K. Wong, and G. Caire, “SD-based low-complexity precoder design for Gaussian MIMO wiretap channels,” in Proc. IEEE Globecom Workshops, Dec. 2022, pp. 612–618.

[19] H. Xu, T. Yang, K.-K. Wong, and G. Caire, “Achievable regions and precoder designs for the multiple access wiretap channels with confidential and open messages,” IEEE J. Sel. Areas Commun., vol. 40, no. 5, pp. 1407–1427, May 2022.

[20] P. J. Schreier and L. L. Scharf, Statistical Signal Processing of Complex-Valued Data: The Theory of Improper and Noncircular Signals. Cambridge, U.K.: Cambridge Univ. Press, 2010.

[21] F. D. Neeser and J. L. Massey, “Proper complex random processes with applications to information theory,” IEEE Trans. Inf. Theory, vol. 39, no. 4, pp. 1293–1302, Jul. 1993.

[22] I. E. Telatar, “Capacity of multi-antenna Gaussian channels,” Eur. Trans. Telecommun., vol. 10, no. 6, pp. 585–595, 1999.
C. Hellings, L. Weiiland, and W. Utschick, “Optimality of proper signaling in Gaussian MIMO broadcast channels with shaping constraints,” in Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP), Florence, Italy, May 2014, pp. 3474–3478.

S. Vishwanath, N. Jindal, and A. Goldsmith, “Duality, achievable rates, and sum-rate capacity of Gaussian MIMO broadcast channels,” IEEE Trans. Inf. Theory, vol. 49, no. 10, pp. 2658–2668, Oct. 2003.

C. Bettilings and W. Utschick, “Improper signaling versus time-sharing in the SISO Z-interference channel,” IEEE Commun. Lett., vol. 21, no. 11, pp. 2432–2435, Nov. 2017.

Y. Zeng, R. Zhang, E. Gunawan, and Y. L. Guan, “Optimized transmission with improper Gaussian signaling in the K-user MISO interference channel,” IEEE Trans. Wireless Commun., vol. 12, no. 12, pp. 6303–6313, Dec. 2013.

C. Hellings and W. Utschick, “Improper signaling versus time-sharing in the two-user Gaussian interference channel with TIN,” IEEE Trans. Inf. Theory, vol. 66, no. 5, pp. 2988–2999, May 2020.

C. Lameiro, I. Santamaria, and P. J. Scharf, “Rate region boundary of the SISO Z-interference channel with improper signaling,” IEEE Trans. Commun., vol. 65, no. 3, pp. 1022–1034, Mar. 2017.

C. Lameiro, I. Santamaria, and P. J. Scharf, “Benefits of improper signaling for underlay cognitive radio,” IEEE Wireless Commun. Lett., vol. 4, no. 1, pp. 22–25, Feb. 2015.

C. Lameiro, I. Santamaria, P. J. Scharf, and W. Utschick, “Maximally improper signaling in underlay MIMO cognitive radio networks,” IEEE Trans. Signal Process., vol. 67, no. 4, pp. 6241–6255, Dec. 2019.

C. Lameiro, I. Santamaria, and P. J. Scharf, “Improper Gaussian signaling for the two-user broadcast channel treating interference as noise,” in Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP), Hong Kong, China, May 2019, pp. 4829–4833.

S. Lagen, A. Argustin, and J. Vidal, “Coexisting linear and widely linear transceivers in the MIMO interference channel,” IEEE Trans. Signal Process., vol. 64, no. 3, pp. 652–664, Feb. 2016.

M. Soleymani, I. Santamaria, and P. J. Scharf, “Improper Gaussian signaling for the K-user MIMO interference channels with hardware impairments,” IEEE Trans. Veh. Technol., vol. 69, no. 10, pp. 16449–16468, Oct. 2020.

Y. Zeng, C. M. Yetis, E. Gunawan, Y. L. Guan, and R. Zhang, “Transmit optimization with improper Gaussian signaling for interference channels,” IEEE Trans. Signal Process., vol. 61, no. 11, pp. 2899–2913, Jun. 2013.

M. Soleymani, C. Lameiro, P. J. Scharf, and I. Santamaria, “Improper signaling for OFDM underlay cognitive radio systems,” in Proc. IEEE Statistical Signal Processing Workshop (SSP), Jun. 2018, pp. 722–726.

B. Ottersten, M. Kristensson, and D. Astely, “Receiver and method for rejecting cochannel interference,” EP Patent EP 1 301 997 B1, Aug. 2005.

R. Meyer, W. H. Gerstacker, R. Schober, and J. B. Huber, “A single antenna interference cancellation algorithm for increased GSM capacity,” IEEE Trans. Wireless Commun., vol. 5, no. 7, pp. 1616–1621, Jul. 2006.

J. T. J. Penttinen, “3GPP mobile communications: GSM,” in The Telecommunications Handbook: Engineering Guidelines for Fixed, Mobile and Satellite Systems. Hoboken, NJ, USA: Wiley, 2013, pp. 281–369.

S. A. Jafar, V. Cadambe, and C. Wang, “Interference alignment with asymmetric complex signaling,” in Proc. 47th Allerton Conf. Commun. Control, Comput. (Allerton), Monticello, IL, USA, Sep. 2009, pp. 991–996.

M. Soleymani, C. Lameiro, I. Santamaria, and P. J. Scharf, “Robust improper signaling for two-user SISO interference channels,” IEEE Trans. Commun., vol. 67, no. 7, pp. 4709–4723, Jul. 2019.

A. A. Nasir, H. D. Tuan, T. Q. Duong, and H. V. Poor, “Improper Gaussian signaling for broadcast interference networks,” IEEE Signal Process. Lett., vol. 26, no. 6, pp. 808–812, Jun. 2019.

M. Gafdar, O. Amin, W. Abedeiseid, and M.-S. Alouini, “Underlay spectrum sharing techniques with in-band full-duplex systems using improper Gaussian signaling,” IEEE Trans. Wireless Commun., vol. 16, no. 1, pp. 235–249, Jan. 2017.

I. Cisszor and J. Korner, “Broadcast channels with confidential messages,” IEEE Trans. Inf. Theory, vol. IT-24, no. 3, pp. 339–348, Mar. 1978.

R. Bustin, R. Liu, H. V. Poor, and S. Shamai (Shitz), “An MMSE approach to the secrecy capacity of the MIMO Gaussian wiretap channel,” in Proc. IEEE Int. Symp. Inf. Theory, Jun. 2009, pp. 2602–2606.

S. Shafiee and S. Ulukus, “Achievable rates in Gaussian MISO channels with secrecy constraints,” in Proc. IEEE Int. Symp. Inf. Theory, Jun. 2007, pp. 2466–2470.

J. Li and A. P. Petropulu, “Optimality of beamforming for secrecy capacity of MIMO wiretap channels,” in Proc. IEEE Int. Workshop Inf. Forensics Secur. (WIFS), Dec. 2012, pp. 276–281.

A. Mukherjee, V. Kumar, E. Jorswieck, B. Ottersten, and L.-N. Tran, “On the optimality of the stationary solution of secrecy rate maximization for MIMO wiretap channel,” IEEE Wireless Commun. Lett., vol. 11, no. 2, pp. 357–361, Feb. 2022.

C. W. K. Lau, C. Nair, and C. Yao, “Uniqueness of local maximizers for some non-convex log-determinant optimization problems using information theory,” in Proc. IEEE Int. Symp. Inf. Theory, Espoo, Finland, Jun. 2022, pp. 432–436.

J. T. Scharf and L. L. Scharf, “Second-order analysis of improper complex random vectors and processes,” IEEE Trans. Signal Process., vol. 51, no. 3, pp. 714–725, Mar. 2003.

Yong Dong (Member, IEEE) received the B.S. and M.S. degrees from Southeast University, Nanjing, China, in 2020 and 2023, respectively. He is currently pursuing the Ph.D. degree with the Department of Electrical Engineering and Computer Science, University of California at Irvine.

Yinfei Xu (Member, IEEE) received the B.E. and Ph.D. degrees in information engineering from Southeast University, Nanjing, China, in 2008 and 2016, respectively. From July 2014 to January 2015, he was a Visiting Student with the Department of Electrical and Computer Engineering, McMaster University, Hamilton, ON, Canada. From March 2016 to July 2017, he was also a Research Assistant and a Post-Doctoral Fellow with the Institute of Network Coding, The Chinese University of Hong Kong, Hong Kong. Since August 2017, he has been with the School of Information Science and Engineering, Southeast University, where he is currently an Associate Professor. His research interests include information theory, wireless communications, and machine learning.

Tong Zhang (Member, IEEE) received the B.S. degree from Northwest University, Xi’an, China, in 2012, the M.S. degree from the Beijing University of Posts and Telecommunications, Beijing, China, in 2015, and the Ph.D. degree in electronic engineering from The Chinese University of Hong Kong, Hong Kong, in 2020. He was a Post-Doc Fellow with the Department of Electrical and Electronic Engineering, Southern University Science and Technology, Shenzhen, China, from 2020 to 2022. He is currently a Lecturer with the Department of Electronic Engineering, Jinan University, Guangzhou, China.

Yili Xia (Member, IEEE) received the B.Eng. degree in information engineering from Southeast University, Nanjing, China, in 2006, the M.Sc. degree (Hons.) in communications and signal processing from the Department of Electrical and Electronic Engineering, Imperial College London, London, U.K., in 2007, and the Ph.D. degree in adaptive signal processing from the Imperial College London in 2011.

Since 2013, he has been an Associate Professor in signal processing with the School of Information Science and Engineering, Southeast University, where he is currently a Full Professor and the Deputy Head of the Department of Information and Signal Processing Engineering. His research interests include complex and hyper-complex statistical analysis, detection and estimation, linear and nonlinear adaptive filters and their applications on communications, and power systems and images. He was a recipient of the Best Student Paper Award at the International Symposium on Neural Networks (ISNN) in 2010 (coauthor) and the Education Innovation Award at the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP) in 2019. He has been an Associate Editor of IEEE TRANSACTIONS ON SIGNAL PROCESSING.