Received April 26, 2018, accepted May 25, 2018, date of publication June 6, 2018, date of current version June 26, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2844458

Intrinsic Secrecy of EGT and MRT Precoders for Proper and Improper Modulations

GUSTAVO ANJOS, DANIEL CASTANHEIRA, ADÃO SILVA, AND ATÍLIO GAMEIRO
Instituto de Telecomunicações and DETI, University of Aveiro, 3810-193 Aveiro, Portugal

Corresponding author: Gustavo Anjos (gustavoanjos@ua.pt)

This work was supported in part by the European Regional Development Fund (FEDER) through the Competitiveness and Internationalization Operational Program (COMPETE 2020) of the Portugal 2020 Framework and in part by FCT/MEC through National funds under Project SWING2 POCI-01-0145-FEDER-016753.

ABSTRACT This paper makes an information theoretical analysis of the intrinsic secrecy level of M-QAM and M-PSK modulation schemes considering the use of equal gain transmission and maximum ratio transmission precoding techniques. In addition to the analysis of the conventional proper M-QAM and M-PSK constellations, a recently proposed family of improper versions of the M-QAM and M-PSK modulation schemes is also evaluated. With the exception of proper M-PSK, which verifies always full secrecy for the considered precoders, the main results show that for low order constellations, the amount of intrinsic secrecy provided by the combination of the precoder and modulation scheme is significant and, therefore, can be exploited in the design of a full secrecy solution. The theoretical derivations provided in this paper can be directly applied to quantify the minimal entropy that a secret key must have to fully secure the exchange of information for these transmission schemes.

INDEX TERMS Physical layer security, improper constellations, M-PSK, M-QAM, channel coherent precoding.

I. INTRODUCTION

The emerging concept of the internet of things (IoT) aims to put billions of regular objects exchanging information in a ubiquitous way using low power wireless transceivers. This massive proliferation of wireless terminals increases the risk of undetectable eavesdropping attacks, bringing new challenges in terms of information secrecy that must be handled by the current and future wireless standards. Furthermore, the continuous evolution of quantum computing is also seen as a serious threat to the current asymmetric cryptographic protocols. In asymmetric public key cryptosystems, the information secrecy is supported by the assumption that the integer factorization of the product of two large prime numbers is a very intensive computational task. However, with the progresses of quantum processing, the factorization of large prime numbers is expected to become feasible in the medium term future, making less secure this kind of cryptographic techniques. The technological advances described above reinforces the need to find new security solutions that can overcome the vulnerabilities associated with current cryptographic protocols [1], [2].

One of the solutions that has received significant attention over the last years is physical layer security, where the achievement of information secrecy is the result of forcing some channel advantage for the legitimate user relatively to the eavesdropper. Therefore, contrarily to what happens with higher layer cryptographic protocols, physical layer security does not rely on the assumption that the eavesdropper has limited computational resources [3]. In wireless communications the randomness of the channels may be used to get this advantage, providing therefore a solution to improve security in these networks.

The fundamentals of information theory to design secure communication channels were formulated by Claude Shannon in 1949. Shannon [4] showed that to reach perfect secrecy it would be required to establish among the legitimate parties a secret key with the same size and entropy of the information source. In his work Shannon did not consider any realistic channel model, assuming that the secret key was the only information not shared among the legitimate nodes and the eavesdropper. A few years later, considering different discrete memory less channels, Wyner [5] showed that when the eavesdropper channel is a degraded version of the legitimate channel, positive secrecy can be reached through coding. The secrecy capacity of the Gaussian wiretap channel was formulated by the first time in [6].

The fundamental knowledge established in these early works paved the way for the development of new and more advanced physical layer secrecy schemes. In recent literature two main lines of research have been followed to advance the state of physical layer secrecy, which are: the coding domain and the signal level domain. In the coding domain the target is design error-correction codes that are also capable to provide some secrecy to the system [7]–[10]. In the signal domain, advanced precoding designs, power allocation schemes, and cooperative jamming based on interference alignment (IA) [11], [12] and artificial noise injection have been proposed in the literature [13]–[18].

The works in [19] and [20] demonstrated that positive secure degrees-of-freedom (DoF) are achieved when several cooperative nodes are available for jamming. To reach the secure DoF, Xie and Ulukus [19], [20] proposed as achievability scheme the use of interference alignment techniques together with discrete M-PAM constellations. Another relevant research topic focus the use of the reciprocal channel characteristic, available in time division duplex (TDD) systems, to establish secure random keys among the legitimate nodes. The potential of received-signal-strength (RSS) measurements and channel phase estimations for key generation is analyzed in [21] and [22]. While some works focus on methods to extract secret keys from the wireless channel, other schemes use those keys to increase the level of randomness in the transmitted data symbols [23], [24]. Anjos *et al.* [23] developed a scheme that maps a secret key, extracted from the reciprocal channel phase, into a discrete M-QAM jamming signal. An alternative solution to the use of jamming signals was suggested in [24] considering the combination of a MRT precoder with a scheme that uses the secret key to apply continuous random phase rotations in the transmitted M-PSK information symbols. As in the pioneering work of Shannon [4], Anjos *et al.* [23] and Chen *et al.* [24] considered secret keys with the same entropy of the information source, not taking advantage or analyzing the intrinsic secrecy already provided by the combination of the channel coherent precoder and the modulation scheme.

Considering precoding, there has been in recent year's significant research on improper Gaussian signaling to efficiently handle interference in complex multiuser scenarios [25]–[27]. The lack of practical application of continuous Gaussian signals led Santamaria *et al.* [28] to develop a family of improper discrete constellations that can be used to approximate the improper Gaussian capacity of a complex AWGN channel. The theoretical analysis done in [28] considered only the legitimate channel capacity for the specific case of improper M-QAM constellations, making the secrecy evaluation of this kind of signals an open issue.

This paper makes an information theoretical analysis of the intrinsic secrecy level of M-QAM and M-PSK modulation schemes considering the use of equal gain transmission (EGT) and maximum ratio transmission (MRT) precoding techniques. Additionally to the analysis of the conventional proper M-QAM and M-PSK constellations, a recently proposed family of improper versions of the M-QAM and M-PSK modulation schemes is also evaluated. With exception of proper M-PSK, which verifies always full secrecy for the considered precoders, the main results show that for low order constellations the amount of intrinsic secrecy provided by the combination of the precoder and modulation scheme is significant, and therefore can be exploited in the design of a full secrecy solution.

The secrecy analysis presented in this work assumes special relevance in TDD systems for scenarios where full blindness regarding the eavesdropper conditions (e.g. channel) is verified. Under such circumstances, most of the works found in the literature consider a two-step encryption process to achieve perfect secrecy. In a first phase, the legitimate terminals extract from the reciprocal channel (TDD) a common secret key with the same entropy of the information source. In a second phase, the channel is secured combining the secret key with the information signal at the legitimate transmitter. However, in future wireless networks, channel coherent precoding will be applied at the physical layer of wireless terminals. As it is demonstrated in the present work, an implicit channel secrecy is naturally obtained when the coherent precoding technique is combined with different modulation schemes (QAM, PSK). Therefore, the analysis of this implicit secrecy is a fundamental work, important not only to quantify how much the entropy requirements of a secret key can be relaxed, but also to understand qualitatively how the signal structure associated to the different modulation schemes impacts the channel secrecy when the considered precoders are applied. To the best of our knowledge, the analysis of the implicit secrecy performed in this manuscript has not been treated in the literature.

Notations: Boldface capital letters denote matrices and boldface lowercase letters denote column vectors. The norm of vector $\mathbf{x}$ is given by $\|\mathbf{x}\|$, being the vector of absolute values of the individual elements of $\mathbf{x}$ defined as $\mathbf{x}_{||}$. The absolute value of the scalar x is defined as $x_{||}$ or $|x|$, while the vector of individual phases of the elements of $\mathbf{x}$ is defined as $\mathbf{x}_{\triangleleft}$. The complex conjugate of x is represented by x^*, while $\Re\{x\}$ and $\Im\{x\}$ are the real and imaginary parts of x. The transpose of vector $\mathbf{x}$ is defined as $\mathbf{x}^T$.

II. SYSTEM MODEL AND EVALUATION METRIC

This section presents the system model as well as the evaluation metrics used to assess the performance of the analyzed constellations.

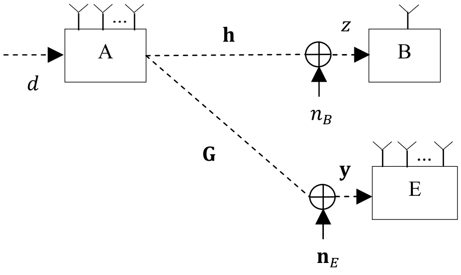

FIGURE 1. General system model.

A. SYSTEM MODEL

The system model considered for the secrecy analysis performed in this work is depicted in Fig. 1. The following nodes compose the system: ‘A’ is the legitimate transmitter (Alice); ‘B’ is the legitimate receiver (Bob); and ‘E’ is the eavesdropper (Eve). We assume that ‘B’ is a single antenna terminal, being ‘E’ and ‘A’ multiple antenna nodes with N_E and N_A elements respectively. In Fig. 1, signal d defines information data that ‘A’ pretends to exchange with terminal ‘B’, the complex vector $\mathbf{h} = [\, h_1 \; h_2 \; \ldots \; h_{N_A} \,]$ represents the channel between ‘A’ and ‘B’, while $\mathbf{G} = [\, \mathbf{g}_1 \; \mathbf{g}_2 \; \ldots \; \mathbf{g}_{N_A} \,]$ is an $N_E \times N_A$ matrix that defines the channel response between node ‘A’ and ‘E’, with $N_E \geq N_A$. The elements of $\mathbf{h}$ and $\mathbf{G}$ are independent complex Gaussian random variables with zero mean and unitary variance. Finally n_B and $\mathbf{n}_E$ represents zero mean complex Gaussian noise with variance equal to σ_B^2 and covariance matrix defined by $\mathbf{U}_E$.

Defining $\mathbf{p}$ as the channel coherent data precoder, the signal transmitted at node ‘A’ is represented as

$$\mathbf{x} = \mathbf{p}d, \tag{1}$$

being the signals received at nodes ‘B’ and ‘E’ formulated as

$$z = \mathbf{h}\mathbf{x} + n_B, \tag{2}$$

$$\mathbf{y} = \mathbf{G}\mathbf{x} + \mathbf{n}_E \tag{3}$$

respectively. We assume that ‘E’ is a passive terminal and has no access to the legitimate channel $\mathbf{h}$, i.e. only $\mathbf{G}$ is known at the eavesdropper. The assumption of a passive eavesdropper means that this node listens the communication and does not cause any intentional interference in the communication channel, making $\mathbf{G}$ unknown to node ‘A’. Furthermore, perfect channel estimation of $\mathbf{h}$ is verified at node ‘A’, being the transmitted power at this node constrained to $E\left[\|\mathbf{x}\|^2\right] \leq 1$. Ideal RF up- and down-conversion is also considered, with all the baseband processing applied to an independent flat fading channel realization.

B. EVALUATION METRIC

As mentioned before, the target of this work is to make an analysis of the intrinsic secrecy of M-PSK and square M-QAM modulations when they are combined with MRT and EGT precoders. In order to quantify the amount of information regarding d that is leaked to node ‘E’, the mutual information $I(d; \mathbf{y})$ is used as a metric. In the secrecy analysis carried in this manuscript we will use the polar decomposition of d and $\mathbf{y}$ to define $I(d; \mathbf{y})$, which is formulated as,

$$\begin{aligned} I(d;\mathbf{y}) = {} & I(d_{||};\mathbf{y}_{||}) + I(d_{\triangleleft};\mathbf{y}_{\triangleleft}|d_{||}) \\ & + I(d_{||};\mathbf{y}_{\triangleleft}|\mathbf{y}_{||}) + I(d_{\triangleleft};\mathbf{y}_{||}|d_{||},\mathbf{y}_{\triangleleft}), \end{aligned} \tag{4}$$

where $d_{||}$ and $\mathbf{y}_{||}$ represent the magnitudes of d and $\mathbf{y}$, while $d_{\triangleleft}$ and $\mathbf{y}_{\triangleleft}$ are the respective phases. The mutual information in (4) can be also defined as

$$I(d;\mathbf{y}) = h(d) - h(d|\mathbf{y}) \tag{5}$$

where $h(d)$ is the entropy of the data source and $h(d|\mathbf{y})$ is the equivocation at the eavesdropper.

III. IMPROPER DISCRETE CONSTELLATION DEFINITION

Contrarily to what happens with proper signals, in improper signal structures the original signal is correlated with the respective complex conjugate. As mentioned before, additionally to the secrecy analysis of the conventional M-PSK and M-QAM constellations, which in this work define the proper constellations, the respective improper versions defined in [28] will be also considered.

The design of the improper discrete family proposed in [28] is done by making a linear transformation of the proper constellation. Considering d as a point in the proper constellation, the corresponding point in the improper constellation is defined in [28] as

$$d_I = w_1 d + w_2 d^*, \tag{6}$$

being the coefficients w_1, w_2 given by

$$w_1 = \sqrt{\frac{1}{2}\,(1+\alpha)}, \tag{7}$$

$$w_2 = \sqrt{\frac{1}{2}\,(1-\alpha)}e^{j\phi}. \tag{8}$$

The phase $\phi \in \left[0;\, \pi/2\right]$ in (8) is a free parameter, while α is computed as

$$\alpha = \sqrt{(1-k^2)} \tag{9}$$

for $k \;\in [0;1]$. The parameter k measures the degree of impropriety, and is defined as

$$k = \frac{\left|\sigma_{dd^*}^2\right|}{\sigma_d^2}, \tag{10}$$

being $\sigma_{dd^*}^2$ the covariance between d and d^*, while σ_d^2 is the variance of d. Two examples of improper constellations generated by the linear transformation defined in (6) are presented in Fig. 2 and Fig. 3 for 256-QAM and 64-PSK.

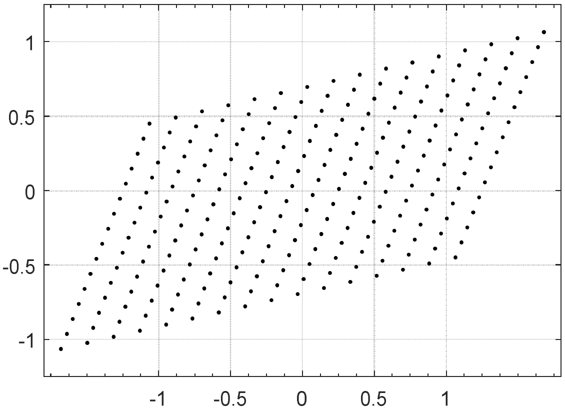

FIGURE 2. **Improper 256-QAM constellation for $k = 0.7$ and $\phi = \pi/4$.**

IV. SECRECY ANALYSIS

This section presents a detailed evaluation of the intrinsic security of proper and improper M-PSK and M-QAM modulations considering that these signals are precoded by coherent techniques such as EGT and MRT. Regarding the

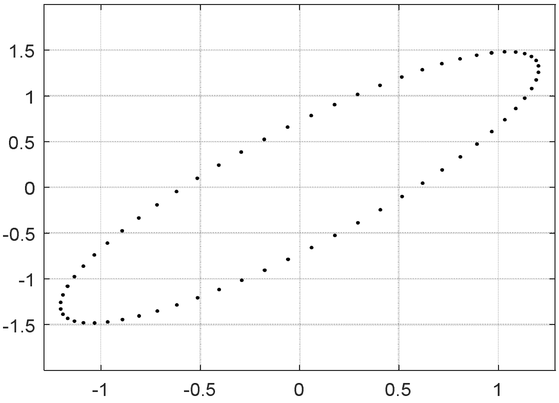

FIGURE 3. Improper 64-PSK constellation for $k = 0.9$ and $\phi = \pi/3$.

M-QAM modulation, our analysis is restricted to the cases where $M = 4^m$, with m a positive integer. The analysis of the secrecy already provided by coherent transmission techniques is a relevant issue since it allow us to quantify the amount of entropy that a shared secret key must have to fully protect information from a malicious eavesdropper.

A. INTRINSIC SECRECY OF COHERENT PRECODING

The intrinsic secrecy of coherent precoding results from the fact that the eavesdropper has no knowledge of the legitimate channel $\mathbf{h}$ that is used in the precoding operation. The secrecy capacity depends on the precoding technique and the specific modulation scheme used to transmit d. In this sub-section we demonstrate how to quantify the leakage of information $I(d; \mathbf{y})$ at node 'E' when both EGT and MRT precoding schemes are applied.

In order to quantify the secrecy obtained only by the combination of the precoder with the modulation scheme, the noiseless regime is considered at node 'E', since this represents a worst case scenario for Bob. In the following, without loss of generality we assume that $\mathbf{G}$ is equalized at the eavesdropper, and therefore

$$\hat{\mathbf{y}} = \mathbf{p}d \tag{11}$$

is the signal observed at terminal 'E', which is used by the eavesdropper to acquire information about the source d in a single realization of the channel.

1) SECRECY ANALYSIS OF EGT PRECODER

In the EGT precoding only the phases of the legitimate channel $\mathbf{h}$ are used in the design of $\mathbf{p}$. Considering the polar representation $h_i = |h_i|\, e^{j\theta_i}, i = 1, 2, \ldots, N_A$, the EGT precoder is defined as

$$\mathbf{p} = \frac{1}{\sqrt{N_A}} \begin{bmatrix} e^{-j\theta_1} & e^{-j\theta_2} & \ldots & e^{-j\theta_{N_A}} \end{bmatrix}^T, \tag{12}$$

being

$$\hat{y}_i = \frac{1}{\sqrt{N_A}} |d| e^{j\theta_d} e^{-j\theta_i} \tag{13}$$

the signals estimated at the eavesdropper with $d = |d|\, e^{j\theta_d}$, the polar representation of d for $i = 1, 2, \ldots, N_A$. Since the channel coefficients in $\mathbf{h}$ follow a complex Gaussian distribution, the phases $\theta_i, i = 1, 2, \ldots, N_A$ are uniformly distributed, which ensures that the information carried in θ_d is protected. Therefore, the amount of information obtained by the eavesdropper when $\hat{\mathbf{y}}$ is observed can be derived from (4) and (5) as,

$$\begin{aligned} I(d; \hat{\mathbf{y}}) &= I(d_{||}; \hat{\mathbf{y}}_{||}) \\ &= h(d_{||}) - h(d_{||}|\hat{\mathbf{y}}_{||}) \\ &= h(d_{||}) \end{aligned} \tag{14}$$

Due to the fact that θ_i is uniform and $\mathbf{h}$ is independent of d, the only term in (4) that is different of zero is $I(d_{||}; \hat{\mathbf{y}}_{||})$. Therefore, as shown in (14), the amount of information that is leaked to the eavesdropper when EGT is applied is quantified by the entropy of the magnitude of the information source d.

2) SECRECY ANALYSIS OF MRT PRECODER

For the case of MRT precoding, the phases and the magnitudes of the legitimate channel $\mathbf{h}$ are used to generate vector $\mathbf{p}$. Considering again the polar definition of $\mathbf{h}$, the precoder is formulated as

$$\mathbf{p} = \frac{1}{\|\mathbf{h}\|} \begin{bmatrix} |h_1|e^{-j\theta_1} & |h_2|e^{-j\theta_2} & \ldots & |h_{N_A}|e^{-j\theta_{N_A}} \end{bmatrix}^T, \tag{15}$$

being

$$\hat{y}_i = \frac{1}{\|\mathbf{h}\|} |d||h_i| e^{j\theta_d} e^{-j\theta_i} \tag{16}$$

the signals acquired at the eavesdropper for $i = 1, 2, \ldots, N_A$. Applying the same arguments used for the EGT case, and considering that the magnitudes $\mathbf{h}_{||}$ of the legitimate channel are known at 'E', an upper bound for the amount of information obtained by the eavesdropper when $\hat{\mathbf{y}}$ is observed can be formulated as,

$$\begin{aligned} I(d; \hat{\mathbf{y}}) &= I(d_{||}; \hat{\mathbf{y}}_{||}) \\ &\leq I(d_{||}; \hat{\mathbf{y}}_{||}|\mathbf{h}_{||}) \\ &= h(d_{||}) - h(d_{||}|\hat{\mathbf{y}}_{||}, \mathbf{h}_{||}) \\ &= h(d_{||}). \end{aligned} \tag{17}$$

The result in (17) shows that when MRT precoding is applied, the entropy of the magnitude of d can also be used to quantify the leakage of information at 'E', however, in this case $h(d_{||})$ defines an upper bound for $I(d; \hat{\mathbf{y}})$.

B. MAGNITUDE ENTROPY OF PROPER CONSTELLATIONS

As demonstrated in Section IV.A, for EGT and MRT precoding the intrinsic secrecy level of the transmission scheme is quantified by the entropy of $d_{||}$, which in turn depends on the structure of the signal constellation applied in the modulation process of d. This sub-section presents a theoretical analysis of $h(d_{||})$ for the conventional M-PSK and square M-QAM modulations. In the following derivations we consider a uniform distribution over the constellation points.

1) M-PSK

In proper M-PSK modulation it's easy to see that all the information is coded in the phase of d, therefore $h(d_{||}) = 0$.

Taking into account (14) and (17),

$$I(d; \hat{\mathbf{y}}) = 0 \tag{18}$$

for both EGT and MRT precoding, i.e. the coherent transmission scheme provides all the secrecy needed to protect information from the eavesdropper, which means that no additional security schemes are required.

2) M-QAM

In square M-QAM constellations, because part of the information is coded in the magnitude of the d, $h(d_{||}) \neq 0$ and some leakage of information is verified at 'E'. In order to quantify the secrecy level of square M-QAM signals, a closed formulation for an upper bound of $h(d_{||})$ is derived as

$$\begin{aligned} h(d_{||}) &\leq u(M) \\ &= \log_2(M) + \frac{2\sqrt{M}}{M} - 3. \end{aligned} \tag{19}$$

The proof regarding the derivation above can be consulted in section A of the Appendix. The result in (19) shows that the amount of information that is protected from the eavesdropper is greater or equal than $\log_2(M) - u(M)$. Additionally, note that $u(M)$ can be used to quantify the minimum entropy that a secret key must have to secure an EGT/MRT transmission scheme when square M-QAM signals are used to modulate d.

The normalized asymptotic analysis of (19) when $M \to \infty$ can be done calculating the following limit,

$$\begin{aligned} \lim_{M\to\infty} \frac{u(M)}{\log_2 M} &= 1 + \frac{2\sqrt{M}}{M\log_2(M)} - \frac{3}{\log_2(M)} \\ &= 1 \end{aligned} \tag{20}$$

The result in (20) shows that when the order M of the square QAM signal grows to infinity, $u(M)$ tends to $\log_2 M$. As the numerical results will also confirm, for $M \to \infty$ the normalized magnitude entropy approaches to one, however, in absolute terms at least three bits are always secured. The analysis presented above shows that there are always some intrinsic secrecy that can be exploited when the considered precoders are applied to proper QAM signals.

C. MAGNITUDE ENTROPY OF IMPROPER CONSTELLATIONS

The entropy of the magnitude component of the improper constellations family described in section III is analyzed in this sub-section. Accordingly to (6), to construct the improper constellation, d_I, the conventional M-PSK and M-QAM constellations are considered for the proper signal d. The first step in this secrecy analysis is to define the general formulation for the magnitude entropy of the improper signal d_I, which is given by

$$\begin{aligned} h(d_{I_{||}}) &= h\left(\sqrt{\Im\{d_I\}^2 + \Re\{d_I\}^2}\right) \\ &= h\left(\Im\{d_I\}^2 + \Re\{d_I\}^2\right) \\ &= h(Q). \end{aligned} \tag{21}$$

The value of Q is derived in section B of Appendix using the complex form of d_I (see section III). The final formulation of Q is defined in equations (22), (23).

$$\begin{aligned} Q = {} & \Re\{d\}^2 + \Im\{d\}^2 \\ & + 2b\Big[\cos(\phi)\left(\Re\{d\}^2 - \Im\{d\}^2\right) \\ & + 2\sin(\phi)\Re\{d\}\Im\{d\}\Big] \end{aligned} \tag{22}$$

$$b = \sqrt{\frac{1}{4}(1-\alpha)(1+\alpha)} \tag{23}$$

In the next two points we will analyze how the entropy of Q is affected when proper M-PSK and M-QAM signals are used for d.

1) IMPROPER M-PSK

Considering d as a proper M-PSK signal, the instantaneous power of d is constant and therefore the value of $\Re\{d\}^2 + \Im\{d\}^2$ does not change. Hence, because

$$\Im\{d\}^2 + \Re\{d\}^2 = K, \tag{24}$$

the value of expression (22) can be simplified to,

$$Q = K + 2bX(\phi) \tag{25}$$

with

$$\begin{aligned} X(\phi) = \cos(\phi)&\left(\Re\{d\}^2 - \Im\{d\}^2\right) \\ &+ 2\sin(\phi)\Re\{d\}\Im\{d\}. \end{aligned} \tag{26}$$

Note that $X(\phi)$ is the only random variable in (25), therefore (21) simplifies to

$$h(d_{I_{||}}) = h[X(\phi)], \tag{27}$$

being $h(d_{I_{||}})$ independent of the impropriety parameter k defined in (10). For an M-PSK constellation, the corresponding real and imaginary parts may be parameterized as follows

$$\Re\{d\} = \cos(\theta_d), \tag{28}$$

$$\Im\{d\} = \sin(\theta_d). \tag{29}$$

Therefore, equation (27) can be re-formulated as

$$h(d_{I_{||}}) = h[\cos(\phi - 2\theta_d)] \tag{30}$$

by replacing (28) and (29) into (26) (see section C.1 of Appendix). Because the angular period of $\cos(\phi - 2\theta_d)$ over θ_d is π, if we consider that M is even and the symbols are uniformly spaced across the phase range, the following bounds

$$\log_2(M) - 2 \leq h[\cos(\phi - 2\theta_d)] \leq \log_2(M) - 1 \tag{31}$$

can be computed for any value of the parameter ϕ (see section C.2 of Appendix). Note that the result in (31) shows that in the worst case the coherent precoding scheme secures at least one bit of d_I, while in the best case at least two bits are secured.

2) IMPROPER M-QAM

In this case, a proper M-QAM signal is used for d in order to generate the improper version d_I formulated in (6) for $0 < \phi < \pi/2$ and $0 < k < 1$. To simplify the explanation of the analysis used for the calculation of the magnitude entropy of d_I, let's begin by consider the equalities in (32)-(34).

$$C = \Re\{d\}^2 + \Im\{d\}^2 \tag{32}$$

$$D = \cos(\phi)\left(\Re\{d\}^2 - \Im\{d\}^2\right) + 2\sin(\phi)\Re\{d\}\Im\{d\} \tag{33}$$

$$Q = C + 2bD \tag{34}$$

To compute $h(Q)$ we start by focusing our attention in D. Since we are considering M-QAM symbols for d, the value of D does not vary among symmetrical symbols, i.e. symbols with the same magnitude and a phase shift of π. Therefore, it is possible to see that considering only the term D, $M/2$ groups of two symmetrical symbols are generated, being the magnitude among the two symbols within each group the same. Depending on the value of ϕ, it can happen that all the groups of two symmetrical symbols generate different values of D among them, which means that $h(Q)$ is fully generated by $h(D)$ and the magnitude entropy is defined as

$$h(Q) = -\log_2\left(\frac{2}{M}\right). \tag{35}$$

For the values of ϕ where exist different groups of symmetrical symbols that generate the same value of D, the value of $h(D)$ is lower, however the groups in which the same value of D is verified have always different magnitudes among them, therefore, when C is added to $2bD$ the value of $h(Q)$ continues to be defined by (35).

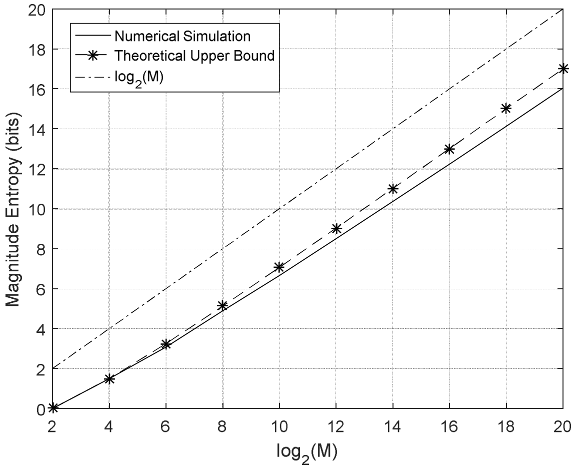

FIGURE 4. Magnitude entropy proper square M-QAM.

V. RESULTS

The theoretical and numerical results for the magnitude entropy of the proper and improper signal constellations analyzed in IV are presented and compared in this section. The magnitude entropy curves in Fig. 4 – Fig. 7 quantify the amount of information in bits per channel use (Bpcu) that is leaked to the eavesdropper when the EGT and MRT channel coherent precoders are used for transmission. As mentioned before, these results can be interpreted as the amount of entropy that a shared secret key must have to force the eavesdropper channel capacity to zero. Therefore, in the following analysis we use as reference the $\log_2(M)$ upper bound, which was defined in [4] as the minimal entropy that must be added to the signal to fully secure a communication channel where the eavesdropper have access to the same signals observed by the legitimate receiver. The difference between the $\log_2(M)$ reference and the obtained results allow us evaluate the amount of secrecy provided by the transmission scheme, i.e. how much the entropy requirements of a secret key can be relaxed (in relation to [4]) when the considered precoders and modulations schemes are applied.

A. PROPER CONSTELLATIONS

In this sub-section only the results regarding proper square M-QAM constellations are discussed, since in proper M-PSK signals the magnitude entropy is always zero.

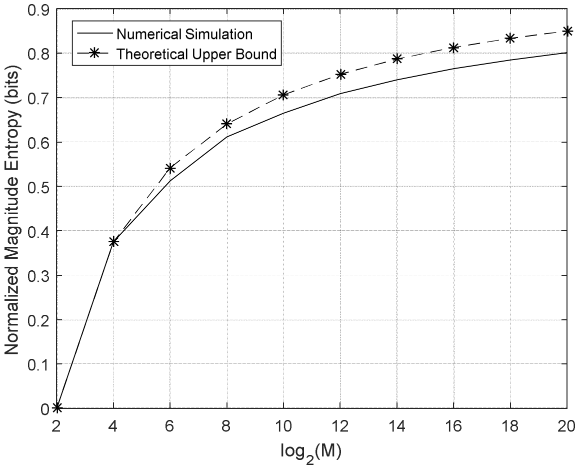

FIGURE 5. Normalized magnitude entropy proper square M-QAM.

The non-normalized magnitude entropy for square M-QAM signals is presented in Fig. 4, while the respective normalized version is depicted in Fig. 5. The first observation is related to the fact that when the constellation order M increases, the percentage of information acquired by the eavesdropper also increases, therefore, as derived in (20) and confirmed by the normalized numerical results in Fig. 5, when $M \rightarrow \infty$ the normalized intrinsic secrecy of the transmission scheme tends to zero. However, for low order constellations the amount of information that is secured by the transmission system is large and therefore can be used to significantly reduce the entropy requirements of a secret key shared between Alice and Bob. Intuitively, these results can be explained by the fact that by increasing the constellation order of a square QAM signal, the cardinality of the set defined by the magnitudes of the constellation increases and therefore more information is leaked for the eavesdropper.

In relation to the theoretical upper bound derived in (19), the results in Fig. 4 and Fig. 5 reveal a good approximation to the value computed numerically.

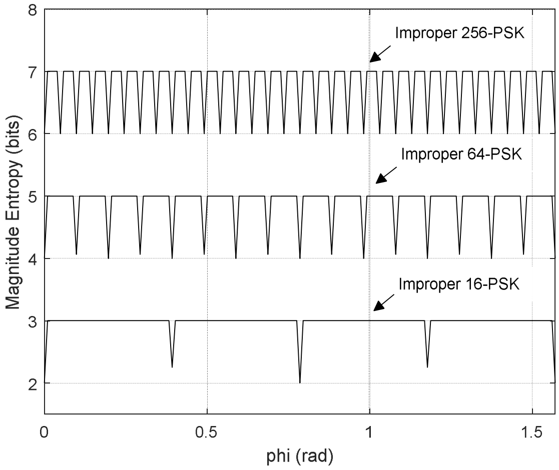

FIGURE 6. **Magnitude entropy improper M-PSK.**

B. IMPROPER CONSTELLATIONS

The entropy results for improper M-PSK signals are presented in Fig. 6. As demonstrated in (24)-(27), the magnitude entropy of improper M-PSK does not depends on the impropriety parameter k, therefore, in this case the analysis was done considering just the variation of the parameter ϕ. As the results in Fig. 6 confirm, depending on the value of ϕ the amount of secured information varies between one and two bits, which agree with the derivation in (31). The maximum entropy values observed in the curves presented in Fig. 6 are a consequence of the fact that for the considered values of ϕ, there are always $M/2$ different magnitudes generated by $M/2$ groups of two constellation points. The minimum values occur when some of the magnitudes generated by these groups coincide, which happen for a finite set of values of ϕ. For some values of this set (e.g. $\pi/4$) we achieve the minimum of equation (31).

In the case of improper square M-QAM, in order to confirm numerically the derivation in (35), we did a sweep in the input parameters ϕ and k considering the ranges $0 < \phi < \pi\big/2$ and $0 < k < 1$, respectively. The numerical evaluation showed that the magnitude entropy of improper square M-QAM only changes with the constellation order M for the considered ranges of ϕ and k, therefore the results in Fig. 7 were presented just as a function of M. As derived in (35), the magnitude entropy results in Fig. 7 allow to conclude that at least one bit is secured for improper M-QAM constellations. As argued before and similarly to the explanation given in the case of improper PSK, these results are due to the fact that for the considered ranges of ϕ and k, there are always $M\big/2$ different magnitude values generated by $M\big/2$ groups of two constellation points. Similarly to the proper square M-QAM signal, when the constellation order increases, the normalized intrinsic secrecy of the transmission scheme reduces with the increase of M. Finally, as it is evident from the results above, the improper versions of the M-PSK and M-QAM modulation schemes have always worst secrecy performance in comparison to the proper case.

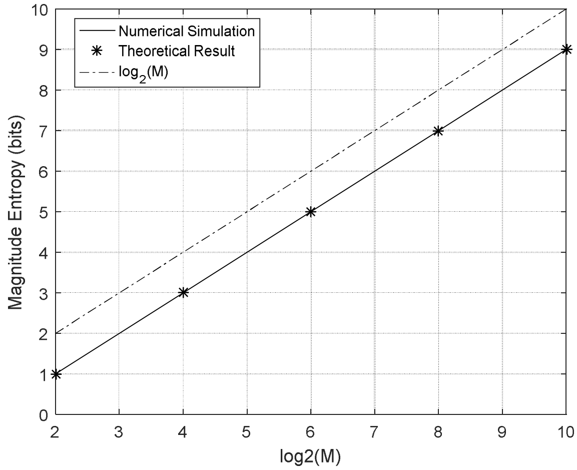

FIGURE 7. **Magnitude entropy improper square M-QAM.**

VI. CONCLUSION

In this work we showed that the proper and improper versions of M-QAM and M-PSK constellations have always associated some intrinsic secrecy when channel coherent precoders like EGT and MRT are applied to these modulation schemes. With exception to proper M-PSK, which verifies always full secrecy, the numerical and theoretical results allowed to conclude that although for large order constellations the normalized secrecy level reduces when $M \rightarrow \infty$, for lower values of M the percentage of information secured by the transmission scheme is large and therefore can be exploited to significantly reduce the entropy of a secret key used to protect the information. Furthermore, a secrecy comparison between the proper and improper constellations showed that the improper case is less secure.

APPENDIX

A. MAGNITUDE ENTROPY OF SQUARE M-QAM

The symmetry observed in a square M-QAM constellation allows to quantify the entropy of the respective magnitude analyzing just the structure of one of the quadrants, more specifically the region $0 < \theta \leq \pi/4$. In the upper bound formulated in (19), it was assumed that each symbol of the constellation within the region $0 < \theta \leq \pi/4$ generates a different magnitude. Furthermore, the constellation symmetry makes that each magnitude referent to the symbols aligned in $\theta = \pi/4$ is generated with probability

$$p_{\pi/4} = \frac{4}{M}, \tag{36}$$

while each of the remaining points in $0 < \theta < \pi/4$ is responsible by generate a magnitude with probability,

$$p_{0,\pi/4} = \frac{8}{M}. \tag{37}$$

Since the number of symbols aligned in $\theta = \pi/4$ and within the region $0 < \theta < \pi/4$ is defined as

$$K_{\pi/4} = \frac{\sqrt{M}}{2}, \tag{38}$$

$$K_{0,\pi/4} = \frac{\left(\sqrt{M}-2\right)\sqrt{M}}{8}, \tag{39}$$

respectively, an upper bound for the magnitude entropy can be computed as

$$\begin{aligned} h(d_{||}) &= -\sum_{d_{||}} p(d_{||})\log_2(d_{||}) \\ &\leq -K_{\pi/4}p_{\pi/4}\log_2\left(p_{\pi/4}\right) \\ &\quad - K_{0,\pi/4}p_{0,\pi/4}\log_2\left(p_{0,\pi/4}\right) \\ &= -\frac{\sqrt{M}}{2}\times\frac{4}{M}\times\log_2\left(\frac{4}{M}\right) \\ &\quad - \left[\frac{\left(\sqrt{M}-2\right)\sqrt{M}}{8}\right]\times\frac{8}{M}\times\log_2\left(\frac{8}{M}\right) \\ &= -\frac{2\sqrt{M}}{M}\log_2\left(\frac{4}{M}\right) \\ &\quad - \left(1-\frac{2\sqrt{M}}{M}\right)\log_2\left(\frac{8}{M}\right) \\ &= \log_2(M) + \frac{2\sqrt{M}}{M} - 3. \end{aligned} \tag{40}$$

In reality, when M is large there are points in the region $0 < \theta < \pi/4$ that generate the same magnitude of a symbol aligned in $\theta = \pi/4$, however, the number of magnitudes in which that overlap is verified is very reduced, making the upper bound derived in (19) a good approximation to the real entropy.

B. MAGNITUDE DERIVATION OF IMPROPER CONSTELLATION

Considering the complex representation of expressions (6)–(8), the improper constellation can be formulated as,

$$d_I = \Re\{d_I\} + j\Im\{d_I\}. \tag{41}$$

with,

$$\Re\{d_I\} = [B + A\cos(\phi)]\,\Re\{d\} + A\sin(\phi)\,\Im\{d\}, \tag{42}$$

$$\Im\{d_I\} = A\sin(\phi)\,\Re\{d\} + [B - A\cos(\phi)]\,\Im\{d\}, \tag{43}$$

$$A = \sqrt{\frac{1}{2}(1-\alpha)}, \tag{44}$$

$$B = \sqrt{\frac{1}{2}(1+\alpha)}, \tag{45}$$

Replacing (42) and (43) in (41), the value of Q is defined as,

$$\begin{aligned} Q &= \Im\{d_I\}^2 + \Re\{d_I\}^2 \\ &= \Im\{d\}^2 + \Re\{d\}^2 \\ &\quad + 2AB\cos(\phi)\left(\Re\{d\}^2 - \Im\{d\}^2\right) \\ &\quad + 4AB\sin(\phi)\,\Re\{d\}\,\Im\{d\} \end{aligned} \tag{46}$$

Finally, since $b = AB$, the formulation in (46) is identical to expression (22).

C. MAGNITUDE ENTROPY OF IMPROPER M-PSK

Some intermediate derivations developed to reach the formulations defined in equations (30) and (31) are presented in the following two points.

1) DERIVATION OF $\cos(\phi - 2\theta_d)$

Replacing (28) and (29) in (26), $X(\phi)$ can be formulated as

$$\begin{aligned} X(\phi) = \cos(\phi)\left[\cos(\theta_d)^2 - \sin(\theta_d)^2\right] \\ + 2\sin(\phi)\cos(\theta_d)\sin(\theta_d). \end{aligned} \tag{47}$$

Then, applying the following trigonometric identities

$$\cos^2(\theta_d) - \sin^2(\theta_d) = \cos(2\theta_d), \tag{48}$$

$$\cos(\theta_d)\sin(\theta_d) = \frac{\sin(2\theta_d)}{2}, \tag{49}$$

expression (47) is defined as

$$X(\phi) = \cos(\phi)\cos(2\theta_d) + \sin(\phi)\sin(2\theta_d). \tag{50}$$

$$\cos(\phi)\cos(2\theta_d) + \sin(\phi)\sin(2\theta_d) = \cos(\phi - 2\theta_d) \tag{51}$$

Replacing (51) in (50), the value of $X(\phi)$ is given by

$$X(\phi) = \cos(\phi - 2\theta_d). \tag{52}$$

2) BOUNDS ON THE ENTROPY OF $\cos(\phi - 2\theta_d)$

Let's start by consider the exponential form of $\cos(\phi - 2\theta_d)$, as follows

$$\cos(\phi - 2\theta_d) = \frac{1}{2}e^{j(\phi-2\theta_d)} + \frac{1}{2}e^{-j(\phi-2\theta_d)}. \tag{53}$$

Considering that Z is a random variable that is generated by the sum of two random variables X and Y, the entropy of

$$Z = X + Y \tag{54}$$

can be formulated as

$$h(Z) = h(X) + h(Y|X) - h(X|Z). \tag{55}$$

Applying (55) to (53), the entropy of $\cos(\phi - 2\theta_d)$ can be written as,

$$\begin{aligned} &h\left[\cos(\phi - 2\theta_d)\right] \\ &= h\left[\frac{1}{2}e^{j(\phi-2\theta_d)}\right] + h\left[\frac{1}{2}e^{-j(\phi-2\theta_d)}\middle|\frac{1}{2}e^{j(\phi-2\theta_d)}\right] \\ &\quad - h\left[\frac{1}{2}e^{j(\phi-2\theta_d)}\middle|\cos(\phi-2\theta_d)\right] \\ &= h(\theta_d) + h(\theta_d|\theta_d) - h\left[\theta_d|\cos(\phi-2\theta_d)\right] \\ &= h(\theta_d) - h\left[\theta_d|\cos(\phi-2\theta_d)\right] \\ &= \log_2(M) - h\left[\theta_d|\cos(\phi-2\theta_d)\right] \end{aligned} \tag{56}$$

Because the angular period of $\cos(\phi - 2\theta_d)$ over θ_d is π, if we consider that M is even and the symbols are uniformly spaced across the phase range, at least there are always groups of two values of θ_d that repeat the same value of $\cos(\phi - 2\theta_d)$. Therefore the following result

$$h\left[\theta_d \,|\, \cos(\phi - 2\theta_d)\right] \geq \log_2(2), \tag{57}$$

defines a lower bound on $h\left[\theta_d \,|\, \cos(\phi - 2\theta_d)\right]$ that occurs when we have $M/2$ groups of two M-PSK symbols generating $M/2$ different values of $\cos(\phi - 2\theta_d)$. Since the maximum number of times that the value of $\cos(\phi - 2\theta_d)$ can be repeated across θ_d is four, an upper bound on $h\left[\theta_d \,|\, \cos(\phi - 2\theta_d)\right]$ is formulated as

$$h\left[\theta_d \,|\, \cos(\phi - 2\theta_d)\right] \leq \log_2(4). \tag{58}$$

The upper bound in (58) occurs when we have $M/4$ groups of four M-PSK symbols generating $M/4$ different values of $\cos(\phi - 2\theta_d)$. Applying (57) and (58) to expression (56), the following bounds are obtained

$$\log_2(M) - 2 \leq h\left[\cos(\phi - 2\theta_d)\right] \leq \log_2(M) - 1. \tag{59}$$

REFERENCES

[1] B. Schneier, "Cryptographic design vulnerabilities," *Computer*, vol. 31, no. 9, pp. 29–33, Sep. 1998.

[2] M. Sandirigama and R. Idamekorala, "Security weaknesses of WEP protocol IEEE 802.11b and enhancing the security with dynamic keys," in *Proc. IEEE Toronto Int. Conf. Sci. Technol. Humanity (TIC-STH)*, Toronto, ON, Canada, Sep. 2009, pp. 433–438.

[3] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 3rd Quart., 2014.

[4] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[5] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1367, Oct. 1975.

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

[7] M. Bloch, M. Hayashi, and A. Thangaraj, "Error-control coding for physical-layer secrecy," *Proc. IEEE*, vol. 103, no. 10, pp. 1725–1746, Oct. 2015.

[8] W. K. Harrison, J. Almeida, M. R. Bloch, S. W. McLaughlin, and J. Barros, "Coding for secrecy: An overview of error-control coding techniques for physical-layer security," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 41–50, Sep. 2013.

[9] D. Sarmento, J. Vilela, W. K. Harrison, and M. Gomes, "Interleaved coding for secrecy with a hidden key," in *Proc. IEEE Globecom Workshop Trusted Commun. Phys. Layer Secur.*, San Diego, CA, USA, Dec. 2015, pp. 1–6.

[10] J. P. Vilela, M. Gomes, W. K. Harrison, D. Sarmento, and F. Dias, "Interleaved concatenated coding for secrecy in the finite blocklength regime," *IEEE Signal Process. Lett.*, vol. 23, no. 3, pp. 356–360, Mar. 2016.

[11] V. R. Cadambe and S. A. Jafar, "Interference alignment and degrees of freedom of the K-user interference channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3425–3441, Aug. 2008.

[12] D. Castanheira, A. Silva, and A. Gameiro, "Retrospective interference alignment: Degrees of freedom scaling with distributed transmitters," *IEEE Trans. Inf. Theory*, vol. 63, no. 3, pp. 1721–1730, Mar. 2017.

[13] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[14] A. L. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process.*, Apr. 2009, pp. 2437–2440.

[15] J. Wang and A. Lee Swindlehurst, "Cooperative jamming in MIMO ad-hoc networks," in *Proc. Conf. Rec. 43rd Asilomar Conf. Signals, Syst. Comput.*, Nov. 2009, pp. 1719–1723.

[16] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "Wireless secrecy regions with friendly jamming," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 256–266, Jun. 2011.

[17] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[18] J. Yang, I.-M. Kim, and D. I. Kim, "Optimal cooperative jamming for multiuser broadcast channel with multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2840–2852, Jun. 2013.

[19] J. Xie and S. Ulukus, "Secure degrees of freedom of the Gaussian wiretap channel with helpers and no eavesdropper CSI: Blind cooperative jamming," in *Proc. Conf. Inf. Sci. Syst.*, Baltimore, MD, USA, Mar. 2013, pp. 1–5.

[20] J. Xie and S. Ulukus, "Secure degrees of freedom of one-hop wireless networks," *IEEE Trans. Inf. Theory*, vol. 60, no. 6, pp. 3359–3378, Jun. 2014.

[21] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Commun.*, vol. 18, no. 4, pp. 6–12, Aug. 2011.

[22] Q. Wang, K. Xu, and K. Ren, "Cooperative secret key generation from phase estimation in narrowband fading channels," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 9, pp. 1666–1674, Oct. 2012.

[23] G. Anjos, D. Castanheira, A. Silva, and A. Gameiro, "Exploiting reciprocal channel estimations for jamming to secure wireless communications," in *Proc. Conf. Wireless Days*, Mar. 2017, pp. 136–142.

[24] B. Chen, C. Zhu, W. Li, J. Wei, V. C. M. Leung, and L. T. Yang, "Original symbol phase rotated secure transmission against powerful massive MIMO eavesdropper," *IEEE Access*, vol. 4, pp. 3016–3025, Jun. 2016.

[25] V. R. Cadambe, S. A. Jafar, and C. Wang, "Interference alignment with asymmetric complex signaling—Settling the Høst–Madsen–Nosratinia conjecture," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4552–4565, Sep. 2010.

[26] Z. K. M. Ho and E. Jorswieck, "Improper Gaussian signaling on the two-user SISO interference channel," *IEEE Trans. Wireless Commun.*, vol. 11, no. 9, pp. 3194–3203, Sep. 2012.

[27] 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.

[28] I. Santamaria, P. M. Crespo, C. Lameiro, and P. J. Schreier, "Information-theoretic analysis of a family of improper discrete constellations," *Entropy*, vol. 20, no. 1, p. 45, 2018.

GUSTAVO ANJOS received the M.Sc. degree in electronics and telecommunications engineering from the University of Aveiro, Aveiro, Portugal, in 2013, where he is currently pursuing the Ph.D. degree in electrical engineering with the Instituto de Telecomunicações. He was with the Instituto de Telecomunicações, where he developed research work in the Flexicell Project—Development of a Multimode/Multiband Remote Radio Header under the context of cloud-radio access network architecture. His current research interests are focused on physical layer security for wireless communications systems.

DANIEL CASTANHEIRA received the Licenciatura (ISCED level 5) and Ph.D. degrees in electronics and telecommunications from the University of Aveiro, Aveiro, Portugal, in 2007 and 2012, respectively. In 2011, he was an Assistant Professor with the Departamento de Eletrónica, Telecomunicações e Informática, University of Aveiro. He is currently an Auxiliary Researcher with the Instituto the Telecomunicações. He has been involved in several national and European Projects, including RETIOT, SWING2, PURE-5GNET, HETCOP, COPWIN, and PHOTON with the FCT Portuguese National Scientific Foundation and CODIV, FUTON, and QOSMOS with the FP7 ICT. His research interests lie in signal processing techniques for digital communications, with an emphasis for physical layer issues, including channel coding, precoding/equalization, and interference cancelation.

ADÃO SILVA received the M.Sc. and Ph.D. degrees in electronics and telecommunications from the University of Aveiro in 2002 and 2007, respectively. He is currently an Assistant Professor with the Department of Electronics, Telecommunications and Informatics, University of Aveiro, and a Senior Researcher with the Instituto de Telecomunicações. He has been participating in several national and European projects, including the ASILUM, MATRICE, and 4MORE with the ICT programme and the FUTON and CODIV projects with the FP7 ICT. He has led several research projects in the broadband wireless communications area at the national level. His interests include multiuser MIMO, multicarrier based systems, cooperative networks, precoding, multiuser detection, massive MIMO and millimeter wave communications. He was a member of the TPC of several international conferences.

ATÍLIO GAMEIRO received the Licenciatura and Ph.D. degrees from the University of Aveiro in 1985 and 1993, respectively. His industrial experience includes a period of one year at BT Labs and one year at NKT Elektronik. He is currently an Associate Professor with the Department of Electronics and Telecommunications, University of Aveiro, and a Researcher with the Instituto de Telecomunicações, Pólo de Aveiro, where he is the head of the group. He has been involved and led IT or University of Aveiro participation on over 20 national and European projects. His current research activities involve space–time–frequency algorithms for the broadband wireless systems and cross-layer design. His main interests lie in signal processing techniques for digital communications and communication protocols, and within this research line, he has done work for optical and mobile communications at the theoretical and experimental level and published over 200 technical papers in international journals and conferences.