Noisy and Dynamic-Index Partitioned Modulation for Physical Layer Security

Lina Mroueh, Idowu Ajayi

Noisy and Dynamic-Index Partitioned Modulation for Physical Layer Security

Lina Mroueh and Idowu Ajayi
Institut Supérieur d'Electronique de Paris, 75006 Paris, France

***Abstract*—In this paper, we propose a noisy and dynamic-Index Partitioned Modulation (IPM) to secure a Quadrature Amplitude Modulation (QAM) constellation transmission over a non-degraded wiretap channel. The QAM is partitioned into multiple disjoint subsets that are separately indexed by a dynamic key, known at the transmitter (Alice) and the legitimate receiver (Bob), but not at the eavesdropper (Eve). The proposed IPM maps the information bits into multiple coded sequences, each one lying in a different partition of the QAM constellation space. This mapping is performed through a cross-bit labeling, that we define to increase the confusion at the eavesdropper, while minimizing the Bit Error Rate (BER) at the legitimate receiver. As the eavesdropper is not aware of the dynamic index pointing to the different partitions, the IPM creates larger Voronoï detection zones around Bob's symbol compared to Eve. To induce further confusion at Eve, we inject random uniform noise into IPM symbols. The noise varies in a domain that is fully included in Bob's larger detection zone, but it exceeds Eve's detection zone. The performances of the noisy IPM scheme in terms of error rate and secrecy rate are analytically and numerically evaluated. Our results show that the IPM scheme creates on the Eavesdropper's link an error floor, independently of its Signal-to-Noise Ratio (SNR). However, the IPM scheme preserves the legitimate link, for which the BER decreases as the SNR increases. Indeed, the secrecy rate remains positive for all SNR values and achieves an asymptotical constant plateau value.**

***Index Terms*—Physical layer security, set partitioning, secrecy rate, symbol error rate rate, non degraded-wiretap channel.**

I. Introduction and Motivations

DESPITE the inherent vulnerabilities of wireless transmission, the last decades have witnessed a significant increase in the amount of sensitive and confidential information exchanged over the wireless interface. This high connectivity has major implications for critical sectors such as healthcare, industry, transportation, and urban infrastructure. However, with this growth in wireless connectivity comes vulnerabilities such as eavesdropping and the extraction of metadata (*e.g.* location, movement). Traditionally, cryptographic techniques at higher protocol layers, have been mainly deployed to protect information against unauthorized access. More recently, a new approach, referred as Physical Layer Security (PLS), has emerged to provide additional resilience against attacks that target the wireless channels. PLS leverages intrinsic wireless channel properties such as noise, fading, and interference to favor a legitimate receiver (Bob) while degrading an eavesdropper (Eve) that attempts to eavesdrop on the communication between a sender (Alice) and Bob [2, 3].

Part of this work is submitted to IEEE Military Communications Conference 2024 [1]. The conference paper presents the concept of Indexed-Partitioned Modulation and provides numerical performances in a coded system.

Several approaches have been adopted in PLS and are broadly categorized as: channel coding [4]–[7], channel adaptation [8]–[10], Artificial Noise (AN) injection [11]–[13], and Physical Layer Encryption [14]. PLS techniques based on channel coding such as lattice codes [4] or Fountain codes [6, 7] are designed for degraded wiretap channel and ensure security by adjusting the coding based on the presumed advantageous legitimate link compared to the eavesdropping link. Considering rateless codes such as Fountain codes in [6, 7], the legitimate SNR link dictates the choice of the number of parity bits. While this number of parity bits is sufficient to decode the signal at Bob, this will not be the case at the eavesdropper with lower SNR than bob. In [4], the difference in the SNR levels is used to design nested lattice pairs with asymmetrical Euclidean distances and densities. The cosets of a high dimensional space are used to label the information, and the transmitted symbol is randomly chosen in the labelled coset space. While the legitimate receiver will be able to decode the noisy symbol within a dense lattice, this will not be the case of the eavesdropper that will experience higher noise level. The degraded wiretap assumption is not suitable when considering eavesdroppers receivers located near legitimate entities with comparable and even better SNR ratios. Channel adaptation techniques exploit the frequency diversity of OFDM systems [11] or the incomplete dimensions of the space generated by multi-antenna systems [12, 13]. For these systems, the security gain depends on perfect knowledge of the radio link and increases significantly with the number of antennas. Most of the AN-based PLS schemes rely on multiple antennas systems in which the AN is injected into the null space of the legitimate user's channel matrix. In highly dynamic environment, the channel estimation requires large amount of feedback, and limits the use of this scheme.

Many of the PLS schemes in the literature have assumed that the channel inputs are Gaussian distributed. The detection complexity of Gaussian signals is high as it takes a continuum of values. In addition to this, the amplitude of Gaussian signals are unbounded, so Gaussian signaling is typically not used in practice [15]. Typically, the channel inputs in practice are usually drawn from a discrete signal constellation such as QAM. These discrete channel inputs help to maintain moderate peak transmission power and receiver complexity. However, finite-alphabet input constraints have a significant impact on the achievable PLS performance and this impact should be taken into account in designing practical PLS schemes.

In this work, we propose a new approach referred as Index Partitioned Modulation (IPM) for communication over a single

input single output *non-degraded wiretap channel*. Our IPM scheme relies on a secret pseudo-random selection of the partition in which lies an information symbol masked by an artificial noise. The common secret dynamic index of sequence is generated at the legitimate entities using a chaotic sequence that is initialized using a common secret seed. The agreement on this common seed is reached at the legitimate entities by quantizing the reciprocal legitimate wireless link in a Time Division Duplex (TDD) system. The spatial decorrelation between the main and wiretap channels ensures independent channel responses, and prevents Eve from accessing the shared secret seed. At each slot, the decoding of noisy symbols is performed in the partitioned subset. However, in the absence of index knowledge at the eavesdropper, decoding is performed using all the constellation space, leading to a smaller detection zone at the eavesdropper than at the legitimate receiver. Inside this partitioned constellation, we propose an optimized labeling, referred as cross-labeling to map the information bits into symbols. This cross-labeling aims to increase the confusion at the eavesdropper and to minimize the BER at the legitimate receiver. To induce more confusion at the eavesdropper, a random uniform AN belonging to a domain space, that is fully included in the large Bob detection zone, is injected. Due to the partitioning, the domain space of the random uniform AN exceeds the eavesdropper detection zone, and this excess leads to a significant degraded decoding at the eavesdropper. The secrecy rate, Symbol Error Rate (SER), and BER at the legitimate receiver and the eavesdropper are analytically derived. Numerical results are finally provided to validate the theoretical results and to demonstrate the secrecy performance and robustness of our scheme.

The rest of this paper is organized as follows. In Section II, we describe the wireless wiretap channel, we introduce our proposed noisy IPM, and we provide a toy example to illustrate our scheme. A mathematical representation is then provided to describe the noiseless IPM, noisy IPM, and the associated proposed cross-labeling in Section III. We evaluate, in Section V, the secrecy rate gap of this scheme, the BER at the eavesdropper and at the legitimate receiver and the robustness of this scheme. Simulation results are presented and discussed in Section VI. Section VII concludes the paper.

Notation: Vectors are denoted by boldface lowercase letters (e.g. $\boldsymbol{x}$) and individual vector elements are denoted by normal letters (e.g. x). $\Re\{.\}$ and $\Im\{.\}$ denote the real and imaginary components of a complex vector/vector element. '$\cap$' and '$\cup$' are used for intersection and union operators on a set while '$\subset$' and '$\emptyset$' show the subsets and nulls in a set. The cardinality of a set is represented by $|.|$ while $\mathbb{E}\{.\}$ and '$\oplus$' represents the expectation and exclusive-OR operators respectively. Finally, the functions $\Phi(.)$ and $\mathcal{Q}(.)$ refer respectively to the cumulative distribution function and the tail distribution of a normal Gaussian variable.

II. Index Partitioned Modulation (IPM): general concept

In this section, we present the general concept of our proposed IPM scheme. The wireless wiretap system model is first presented in Subsection II-A. Next, we describe in Subsection II-B and II-C the main concepts of noiseless IPM and noisy IPM. Finally, toy examples illustrating noiseless and noisy IPM concepts are provided in Subsection II-D.

A. Wireless wiretap channel

We consider a Single Input Single Ouptut (SISO) wireless channel in which Alice sends a symbol x to Bob, that is subject to a power constraint $\mathbb{E}[|x|^2] = P$ with P being the total power at the transmitter. The transmitted signal is intercepted by an eavesdropper having a single antenna, situated in the proximity of the legitimate receiver. We assume that Bob's channel is independent of Eve's one, which can be satisfied when the two receivers are separated by at least half a wavelength [16, 17]. Each receiver estimates its channel coefficient, and the modulus of each channel is assumed as i.i.d. random Rayleigh distributed variable. The received signals at Bob and Eve are,

$$y^{(b)} = h^{(b)}x + z^{(b)}, \quad (1)$$

$$y^{(e)} = h^{(e)}x + z^{(e)}. \quad (2)$$

The transmitted signal at Alice is denoted by x, the received signals at Bob and Eve are respectively $y^{(b)}$ and $y^{(e)}$. The random noise $z^{(b)}$ and $z^{(e)}$ are i.i.d. Gaussian complex variables with zero mean and respective variances of σ_b and σ_e. The average $\mathrm{SNR}^{(b)}$ and $\mathrm{SNR}^{(e)}$ at Bob and Eve are defined as,

$$\mathrm{SNR}^{(b)} \triangleq \frac{P}{2\sigma_b^2}, \quad \mathrm{SNR}^{(e)} \triangleq \frac{P}{2\sigma_e^2}. \quad (3)$$

B. General IPM concept

Our proposed IPM scheme is illustrated in Figure 1 and consists of partitioning the 2^q-QAM modulation (denoted by Ω_c with $|\Omega_c| = 2^q$) into 2^ℓ multiple disjoint spaces (denoted by $\Lambda_m \subset \Omega_c$, with $1 \leq m \leq 2^\ell$), such that: $\Lambda_m \cap \Lambda_n = \emptyset \ \forall m, n$; $\bigcup_m \Lambda_m = \Omega_c$ and $|\Lambda_m| = 2^{q-\ell}$. Each sub-space

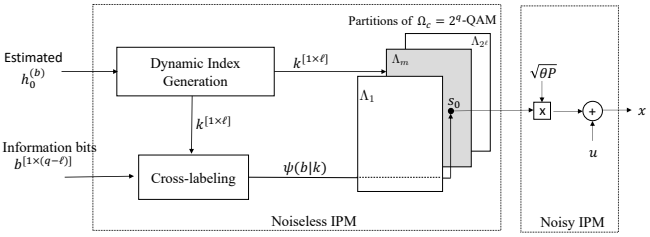


Fig. 1: The dynamic index and the cross-labeling respectively indicate the partition (in gray) and the QAM symbol inside this partition. The signal-output is the noisy IPM x in (5).

Λ_m is indexed at Alice side, by a dynamically chosen index $\boldsymbol{k}$ with length ℓ. A given $(q-\ell)$ information bits sequence $\boldsymbol{b}$ will have different images in Ω_c depending on the value of the index $\boldsymbol{k}$. At Alice side, the index $\boldsymbol{k}$ will dictate the reduced sub-space Λ_m. To map the bits into non-normalized QAM symbols $\psi(\boldsymbol{b}|\boldsymbol{k})$, a cross-labeling is proposed to induce confusion at Eve side while minimizing the Hamming distance

between neighboring symbol at the legitimate receiver. We let s_0 be the corresponding normalized QAM symbol such that

$$s_0 = \frac{1}{\sqrt{E_s}}\psi(\boldsymbol{b}|\boldsymbol{k}) \tag{4}$$

where $\psi(\boldsymbol{b}|\boldsymbol{k})$ is the cross-labeling mapping function and $E_s = \frac{2(2^q-1)}{3}$ is the QAM symbol energy.

C. Noisy IPM

In the high SNR regime, the Euclidean distances between neighboring points are relatively large in both lattices Λ_m or Ω_c. In this case, the secrecy gain becomes non-significant as the noisy symbols become distinguishable at Bob as well as at Eve. To induce more confusion at the eavesdropper, we propose to inject a random noise, denoted as u, into the QAM symbol generated by the IPM. To satisfy the power constraint, a scaling factor $0 \leq \theta \leq 1$ is used to split the power between the useful information and the artificial noise such that $\mathbb{E}[|u|^2] = (1-\theta)P$. The noisy IPM signal generated at Alice side is then,

$$x = \sqrt{\theta P}s_0 + u. \tag{5}$$

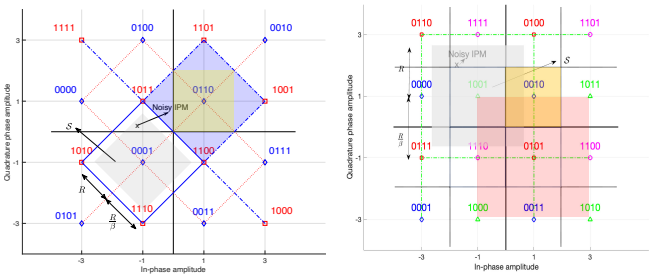
The pdf of this random uniform AN and the value of θ will be further detailed in Subsection II-D2.

D. Toy example illustrating the IPM concept

To illustrate our proposed scheme, we provide the following examples of one-bit and two-bits partitioning with noiseless IPM and noisy IPM.

1) Noiseless IPM: We consider a 16-QAM constellation with 2 partitions in Figure 2a and 4 partitions in Figure 2b. The last three (resp. the two) bits in Figure 2a (resp. Figure 2b) are the information bits and the first (resp. the first two) bits corresponds to the shared dynamic index between Alice and Bob. As an example in Figure 2a, the image of the information sequence 101 is $\psi(101|0) = -3-3i$ if the index is 0, and is equal to $\psi(101|1) = 1+3i$ if the index is 1. This means that the sequence 101 has two distinct images in the constellation of Eve Ω_c. For the 2-bit partitioning example in Figure 2b, $\psi(00|00) = -3+1i$, $\psi(00|01) = 1+3i$, $\psi(00|10) = -1-3i$ and $\psi(00|11) = 3-1i$.

2) Noisy IPM: Figure 2a illustrates Bob detection zones (or the Voronoï regions around each symbol) of a 16-QAM with two partitions: the blue lines delimit the detection zones in the partition with index 0 and the red ones for the case of an index 1. The symbol detection is performed without error as far as the received symbol remains in the detection zone around the transmitted QAM symbol, to say $\psi(001|0) = -1-1i$. To induce more confusion at Eve, we propose to transmit, instead of the IPM QAM symbol, a random complex number uniformly chosen in the gray square $\mathcal{S}$ (that is included in the Voronoï region) centered around this transmitted symbol. We can intuitively observe that, at Eve, depending on the position of the received symbol, there is an equal probability that this noisy IPM symbol stems from the transmitted symbol and its neighboring symbols (*e.g.* $-1-1i$ or $-1+1i$ for the noisy IPM signal in Figure 2a). In a similar way, Figure 2b illustrates Bob's detection zones with 4 partitions. Here again, instead of transmitting a QAM symbol (to say $\psi(01|10) = -1+1i$), we add random uniform AN $\in \mathcal{S}$ around this point (in gray).



(a) Noisy IPM: one-bit partitioning (b) Noisy IPM: two-bit partitioning

Fig. 2: 16QAM IPM. Fig. (2a): In Λ_{00}, the Voronoi region around $1+1i$ is in blue; In Ω_c, it is in yellow. Fig. (2b): In Ω_c, the Voronoi region around $1+1i$ is in yellow. In Λ_{01}, the Voronoi region centered around $-1-1i$ is in red.

III. Design of Noisy IPM Encoder

In this section, we detail the different transmitter blocks of Figure 1. Subsection III-A and III-B describes the IPM partitioning and bit mapping referred as cross-labeling. The AN is then characterized in Subsection III-C. Finally, we provide in Subsection III-D the channel dependent index generation algorithm.

A. 2^q-QAM partitioning

The partition concept is known since the seminal work on mapping by set partitioning of Ungerboëck in [18] that combines coding and modulation in a single unit to mitigate the noise impact on the digital received signal. Unlike the original Ungerboëck partitioning scheme, we assume here that the legitimate receiver has full knowledge of the index-partition. Moreover, the objective of the bit labeling in IPM scheme is different from the mapping by set partitioning. It aims to induce more error at the eavesdropper, and to minimize the error at the legitimate receiver. The main idea of the partitioning is to recursively divide the symbols in the 2^q-QAM constellation into two groups of disjoint symbols. In each group of symbols, the Euclidean distance between the neighboring points is increased. For an IPM with 2 (resp. 4) partitions corresponding to an index-length of $\ell = 1$ (resp. $\ell = 2$), the minimal Euclidian distance in Figure 3 (resp. Figure 4) is $d_{\min}\sqrt{2}$ (resp. $2d_{\min}$) where $d_{\min}$ is the minimal distance in the normalized QAM constellation with $d_{\min} = \frac{2}{\sqrt{E_s}}$. In the general case, the power scaled minimal distance in a given partition with ℓ bits is

$$d_{\mathbb{E}}(\Lambda_k) = 2^{\ell/2}\sqrt{\theta P}d_{\min}. \tag{6}$$

To easily generate the partitions for $\ell = 1$ and $\ell = 2$, one can consider the 2^q-QAM constellation as the set of points generated by $4\mathbb{Z}[i] - (2+2i) + (\pm 1 \pm 1i)$ (inside the constellation bounds). Note that in each case, $(\pm 1 \pm 1i)$ generates shifts with 4 orientations $\swarrow\nearrow\nwarrow\searrow$ around $4\mathbb{Z}[i] - (2+2i)$

points. For the two partitions case, Λ_0 (resp. Λ_1) are generated considering $\swarrow\nearrow$ (resp.$\nwarrow\searrow$) orientations shifts. For the 4 partitions case, the partitions Λ_{00}, Λ_{01}, Λ_{10} and Λ_{11} are generated considering $\swarrow, \nearrow, \nwarrow, \searrow$ orientations respectively. For 2^q-QAM constellation, the average number of neighboring symbols at Bob side for $\ell = 1$ and $\ell = 2$ is respectively,

$$\bar{N}_1^{(b)} = 4(1 - 2^{-q/2})^2, \quad (7)$$

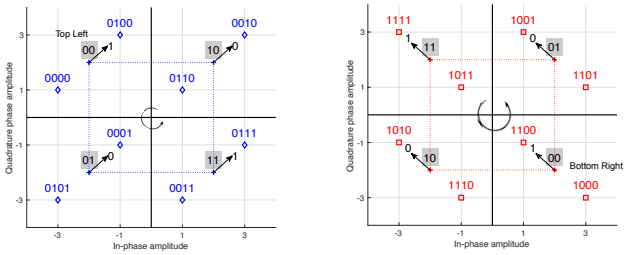
$$\bar{N}_2^{(b)} = 4(1 - 2^{-(q-2)/2}). \quad (8)$$

At the eavesdropper, the average number of neighboring symbols $\bar{N}^{(e)}$ computed in Ω_c is,

$$\bar{N}^{(e)} = 4(1 - 2^{-q/2}). \quad (9)$$

B. Cross-labeling: bit mapping in the partitioned 2^q-QAM

Let $\boldsymbol{b}$ be the information bit vector carrying $(q-\ell)$ bits and $\boldsymbol{k}$ be the index partition of $1 \leq \ell \leq 2$ bits. Each symbol in the 2^q-QAM constellation is labeled by the binary sequence $[\boldsymbol{k}, \boldsymbol{b}]$. Knowing $\boldsymbol{k}$, the bit mapping is a bijection, and $\boldsymbol{b}$ has a unique image denoted $\psi(\boldsymbol{b}|\boldsymbol{k})$. However, when $\boldsymbol{k}$ is not known, $\boldsymbol{b}$ has 2^ℓ images in Ω_c with $\vec{\psi}(\boldsymbol{b}) = \big(\psi(\boldsymbol{b}|\boldsymbol{k}_1), \ldots, \psi(\boldsymbol{b}|\boldsymbol{k}_{2^\ell})\big)$. For the ℓ-bit length index k, the bit labeling is performed to guarantee that: (1) the Euclidean distance between all the images of $\psi(\boldsymbol{b})$ is maximized; (2) the Hamming distance between the information sequence (the $q-\ell$ last bits) considering two neighboring symbols in Ω_c is at least equal to 1; (3) the Hamming distance between the information sequence in Λ_k is minimized. The first two conditions will increase the confusion at the eavesdropper when attempting to decode the sequence $\boldsymbol{b}$ in Ω_c. The last condition will minimize Bob's BER.



(a) IPM: $\Lambda_0 \rightarrow \diamond$ (b) IPM: $\Lambda_1 \rightarrow \square$.

Fig. 3: Binary mapping with respect to $\mathcal{M}_1(k)$ in (10)

1) Cross-labeling with one-bit index: In this case, we need to label the points generated by the shifted $4\mathbb{Z}[i]-(2+2i)$ with a shift orientation of $\swarrow\nearrow$ for $k=0$, and $\nwarrow\searrow$ for $k=1$. The information sequence consists of $(q-1)$ bits. Our proposed cross-labeling is performed in 4 steps: (S1) Identify inside each partition Λ_k, the virtual points generated by $4\mathbb{Z}[i] - (2+2i)$ and situated inside the constellation. These virtual points are the same in both partitions but the bit-labeling is different. (S2) To label these virtual points, a Gray mapping $\mathcal{M}_1(k)$ is used with a sense defined with respect to k and the all-zero sequence of $(q-2)$ bits as,

$$\mathcal{M}_1(k) = \begin{cases} \text{top-left } \vec{0} \text{ ; anti-clockwise Gray map,} & k=0, \\ \text{bottom-right } \vec{0} \text{ ; anti-clockwise Gray map,} & k=1. \end{cases} \quad (10)$$

(S3) In each partition, the shift orientation $\nearrow$ in Λ_0 (resp. $\nwarrow$ in Λ_1) is alternatively labeled by 1 and 0. (S4) The QAM symbol is labeled from left to right by: the partition index, the shift direction binary label, and the virtual point label.

Our proposed bit labeling is illustrated in Figure 3 : Virtual points are indicated in Figure 3a and 3b and are labeled according to (10).

2) Cross-labeling for two-bits index partitioning: In this case, the partition is determined based on the shift orientation $00 = \swarrow, 01 = \nearrow, 11 = \nwarrow, 10 = \searrow$. Similarly, the virtual points are identified and are labeled with respect to the position of the $(q-2)$-length zero sequence and the sense of the gray mapping $\mathcal{M}_2(\boldsymbol{k})$ is,

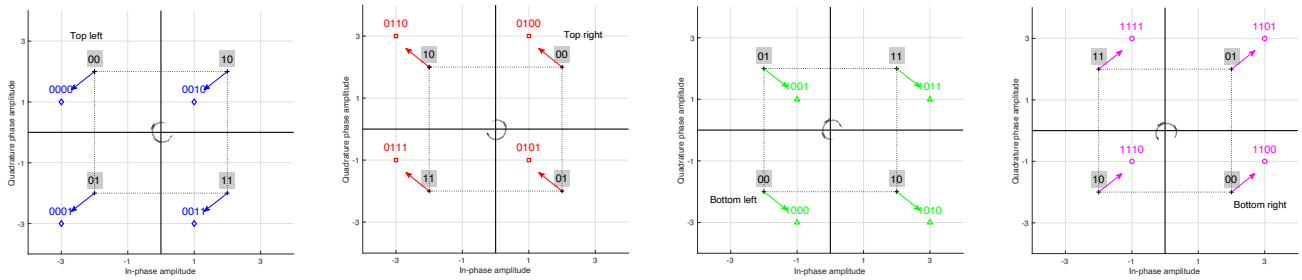
$$\mathcal{M}_2(\boldsymbol{k}) = \begin{cases} \text{top-left } \vec{0}\text{; anti-clockwise Gray map,} & \boldsymbol{k}=00, \\ \text{top-right } \vec{0}\text{; clockwise Gray map,} & \boldsymbol{k}=01, \\ \text{bottom-left } \vec{0}\text{; clockwise Gray map,} & \boldsymbol{k}=10, \\ \text{bottom-right } \vec{0}\text{; anti-clockwise Gray map,} & \boldsymbol{k}=11. \end{cases} \quad (11)$$

Figure 4 illustrates the 16-QAM bit labeling with a bit index of length 2. The virtual points in Figures 4a to 4d are identified and labeled according to (11).

The average Hamming distance and the average number of neighboring symbols are summarized in Table I.

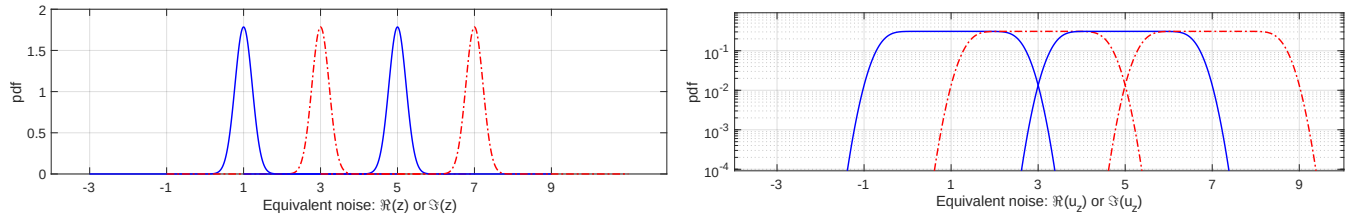
C. Artificial noise characteristics

To simplify the notation, we drop all Bob and Eve superscripts $^{(b)}$ and $^{(e)}$ from the output, the input and channels. The



(a) Λ_{00} (b) Λ_{01} (c) Λ_{10} (d) Λ_{11}

Fig. 4: Binary mapping with respect to $\mathcal{M}_2(k)$ in (11)



(a) Gaussian noise (b) Equivalent noise

Fig. 5: 1D illustration of the equivalent noise: 1 and 3 are neighboring points in Ω_c with Voronoï region $]-2;+2[$ and $]-4;+4[$; 1 and 5 are neighboring in a given partition with larger Voronoï regions $]-3;+3[$ and $]+3;+7[$.

TABLE I: Cross-labeling: average Hamming distance

		64-QAM		16QAM		QPSK
	ℓ	1	2	1	2	1
Bob	$d_{\mathbb{H}}$	1.37	1	1.23	1	1
	$\bar{N}$	3.06	3	2.25	2	1
Eve	$d_{\mathbb{H}}$	2.65	1.43	2.17	1.34	0.5
	$\bar{N}$	3.5	3.5	3	3	2

model in (1), (2) and (5) becomes,

$$y = \sqrt{\theta P} h s_0 + (hu + z). \tag{12}$$

1) Characterization of the AN distribution: The equivalent noise $u_z = u + h^{-1}z$ in (12) is the sum of the AN u and a Gaussian random variable $h^{-1}z \sim \mathcal{CN}(0, \sigma_h)$ with $\sigma_h = \sigma/|h|$. The pdf of the sum is nothing but the convolution of the pdf of u with the Gaussian distribution. In the high SNR regime, the pdf of u should preserve the quality on the legitimate link, and induce confusion at the eavesdropper. To perform this, the pdf of u needs to convert the Gaussian distributed noise illustrated in Figure 5a into a flat-topped distributed variable on the edges of Ω_c-Voronoï region, but with a thin-tail at the edge of Λ_m-Voronoï region as illustrated in Figure 5b. The flat-topped behavior of the distribution ensures confusion between neighboring points of Ω_c, however, the thin-tail behavior of the equivalent noise makes the two neighboring points of Λ_m distinguishable as illustrated in Figure 5b. When $\sigma = 0$, the Gaussian distribution converges to a dirac and the required behavior in Figure 5b converges to a window with width R that should be set in a judicious manner. To regularize the thickness of the tail in the Λ_m-Voronoï region and the flat-topped behavior in Ω_c-Voronoï region, the uniform noise bounds are set to $\pm R$ where,

$$R \triangleq \beta d_{\mathbb{E}}(\Lambda_k)/2 = \sqrt{\theta P} 2^{\ell/2-1} \beta d_{\min} \tag{13}$$

with $d_{\mathbb{E}}(\Lambda_k)$ is defined in (6) and $0 \leq \beta \leq 1$ is a regularization parameter that ensures that the AN does not exceed Λ_m - Voronoï region. The 2D-pdf of the AN is then,

$$f(u) = \begin{cases} \frac{1}{|\mathcal{S}|} & u \in \mathcal{S} \\ 0 & \text{otherwise} \end{cases} \tag{14}$$

$$\mathcal{S} = \{u \in \mathbb{C} : -R \leq \Re(u), \Im(u) \leq R\}, \tag{15}$$

is defined in the $\pi/4$**-rotated coordinate system** for $\ell = 1$, and in the **Cartesian coordinate system** for $\ell = 2$, and its area is $|\mathcal{S}| = 4R^2$.

2) Power control of AN: The AN power computed in the Cartesian coordinate system for $\ell = 2$ and the $\pi/4$-rotated coordinate system for $\ell = 1$ is $\mathbb{E}[|u|^2] = \frac{2R^2}{3}$. The power constraint, satisfied for $\mathbb{E}[|u|^2] = (1-\theta)P$, requires that,

$$\theta = \frac{3E_s}{3E_s + 2^{\ell+1}\beta^2}. \tag{16}$$

D. Dynamic shared index generation

IPM relies essentially on a dynamic index that indicates, for Alice and Bob, in which partition the QAM symbol lies. This index should change dynamically in each transmission slot to guarantee that it is not intercepted at the eavesdropper.

1) Common seed generation: To perform this, a common seed $0 < \alpha_0 < 1$ is generated at the beginning of the transmission based on the impulse response of the TDD channel between Alice and Bob. The key establishment technique based on channel reciprocity-based has been widely investigated in literature aiming to generate a key [14, 20]. Our goal is to use this partial quantized knowledge to generate a shared common seed at Alice and Bob. A quantization of the channel between Alice and Bob is required to generate this common seed over a large number of bits, to say 128 bits or 256 bits as in [19]. The agreement generation of the binary sequence extracted from the quantized channel include four steps: channel probing, channel quantization, information reconciliation and privacy amplification. We assume that this common seed is not available at Eve, and that 2^{128} or 2^{256} trials are required to know the exact initial seed.

2) Dynamic index generation: To generate the dynamic index at each slot, we use the chaotic sequence [21] that critically depends on its initial value and the μ-value with $\mu \in [0, 4]$. Note that the chaotic behavior of the sequence occurs when initiating μ to a value $\mu > 3.57$ (except for some values around 3.82 where there is an oscillation around 5 distinct values). The main steps of the dynamic index generation are illustrated in Algorithm1. Moreover, this common seed is not sent on the wireless interface, and a congruential Pseudo-Random Number Generator (PRNG) is used to generate bits associated to the chaotic sequence output (line 7 in Algorithm 1). This operation is not reversible and it will not be possible to find the values of α_t in the algorithm from the index k_t. Using a numerical simulation, we have shown that this chaotic-sequence algorithm provides an equal probability to generate a bit equal to 1 or 0.

Algorithm 1 Generation of dynamic index

Require: The time slot t, the length of the index ℓ

Set the precision parameter to $p = 12$
Set $\mu_0 = 3.7$
if t = 0 **then**
    α_0 = INITIALIZE LOGISTIC MAP($\boldsymbol{h}^{(b)}$)
end if
$\alpha_t = \mu\alpha_{t-1}(1-\alpha_{t-1})$
Compute $\bar{\alpha}_t = \text{round}(\alpha_t \times 10^p) \pmod{2^\ell}$
Convert $\bar{\alpha}_t$ to binary: $\boldsymbol{k}_t = \text{decimal to binary}(\bar{\alpha}_t, \ell)$
Save the value of α_t

IV. Design of noisy IPM Decoder

In this section, we convey the maximum likelihood decoding criterion into an Euclidean distance minimization. For this, we characterize first the equivalent total noise distribution and deduce the symbol decoding rule.

A. Equivalent total noise distribution

Given the channel model in (12), the conditional probability of y given s_0, denoted as $\omega(y|s_0,h)$ is computed in Lemma 1.

Lemma 1. *For the noisy IPM case, the conditional probability $\omega(y|s_0,h)$ is*

$$\omega(y|s_0,h)=\frac{1}{4R^2}\prod_{k=1}^{2}\left[\Phi\Big(\frac{R-u_{z,k}^{(\ell)}}{\sigma_h}\Big)-\Phi\Big(-\frac{R+u_{z,k}^{(\ell)}}{\sigma_h}\Big)\right] \tag{17}$$

with $(u_{z,1}^{(1)}, u_{z,2}^{(1)})$ are the coordinates of

$$u_z = h^{-1}y - \sqrt{\theta P}s_0, \qquad |h| \neq 0, \tag{18}$$

in the $\pi/4$-rotated coordinate system, and $(u_{z,1}^{(2)}, u_{z,2}^{(2)})$ are the coordinates of u_z in the Cartesian coordinate system, such that, $u_{z,1}^{(2)} = \Re(u_z)$, $u_{z,2}^{(2)} = \Im(u_z)$ and $u_{z,1}^{(1)} = \cos(\pi/4)u_{z,1} + \sin(\pi/4)u_{z,2}$ and $u_{z,2}^{(1)} = -\sin(\pi/4)u_{z,1} + \cos(\pi/4)u_{z,2}$.

Proof. The proof is provided in Appendix A. □

B. Maximuml-Likelihood (ML) criterion and detection zone

Theorem 2 summarizes the IPM decoding rules obtained by applying the ML criterion to Lemma 1.

Lemma 2 (ML detection)**.** *The ML detection $\max\omega(y|s,h)$ is equivalent to finding the constellation point that minimizes the Euclidean distance in the appropriate Lattice $\mathcal{L}$, i.e.,*

$$\hat{s} = \arg\min_{s\in\mathcal{L}} |y - \sqrt{\theta P}hs|^2. \tag{19}$$

where $\mathcal{L} = \Lambda_k$ is the partition indexed by k at the legitimate receiver and $\mathcal{L} = \Omega_c$ is the 2^q-QAM at the eavesdropper.

Proof. The proof is provided in Appendix B. □

V. Secrecy Metrics Evaluation

In this section, we evaluate the secrecy performance of our scheme in terms of secrecy rate in Subsection V-A and error rate in Subsection V-B, as well as its robustness against attacks in Subsection V-C.

A. Secrecy rate evaluation

In this subsection, we compute in Theorem 1 the secrecy rate defined as the difference in mutual information between the legitimate link and the eavesdropper's link with discrete and finite alphabet inputs. The main difference between both links stems from the knowledge of the initial value of the dynamic index at Bob side but not at Eve.

Theorem 1 (Mutual information)**.** *The mutual information with full index knowledge,*

$$I(\psi(\boldsymbol{b}|\boldsymbol{k}), y^{(b)})=(q-\ell) - \mathbb{E}\left[\log_2 \frac{\sum_{s_0\in\Lambda_{\boldsymbol{k}}}\omega(y^{(b)}|s_0,h^{(b)})}{\omega(y^{(b)}|\psi(\boldsymbol{b}|\boldsymbol{k}),h^{(b)})}\right], \tag{20}$$

and the mutual information without index knowledge,

$$I(\psi(\boldsymbol{b}), y^{(e)}) = (q-\ell) - \mathbb{E}\left[\log_2 \frac{\sum_{s_0\in\Omega_c}\omega(y^{(e)}|s_0,h^{(e)})}{\sum_{\boldsymbol{k}}\omega(y^{(e)}|\psi(\boldsymbol{b}|\boldsymbol{k}),h^{(e)})}\right]. \tag{21}$$

The Secrecy Rate (SR) is computed using (20) and (21). as,

$$SR = I_b(\psi(\boldsymbol{b}|\boldsymbol{k}), y^{(b)}) - I_e(\psi(\boldsymbol{b}), y^{(e)}).$$

Proof. The proof is provided in Appendix C. □

Corollary 1.1 (Secrecy rate asymptotic behavior)**.** *In the high SNR regime, the asymptotic mutual information of the legitimate link between Alice and Bob is,*

$$\lim_{\sigma\to 0} I_b(\psi(\boldsymbol{b}|\boldsymbol{k}), y^{(b)}) = (q-\ell). \tag{22}$$

The asymptotic mutual information of the eavesdropper link between Alice and Eve is,

$$\lim_{\sigma\to 0} I_e(\psi(\boldsymbol{b}), y^{(e)}) = (q-\ell) - SR_e(\beta) \tag{23}$$

with $SR_e(\beta) = 0$ if $0 < \beta \leq \frac{1}{2}$. Otherwise, for the 2^q-QAM constellation with $q \neq 2$,

$$SR_e(\beta) = \begin{cases} \bar{N}^{(e)}\left(1-\frac{1}{2\beta}\right)^2, & \ell = 1 \\ \bar{N}^{(e)}\left(1-\frac{1}{2\beta}\right) - \frac{1}{2^{q-2}}\left(1-\frac{1}{2\beta}\right)^2 & \ell = 2, \end{cases} \tag{24}$$

with $\bar{N}^{(e)}$ being the average number of neighbors around each constellation point in Ω_c defined in (9). For the case of QPSK with $\ell = 1$-bit partitioning,

$$SR(\beta) = \left(1-\frac{1}{2\beta}\right)^2.$$

Proof. The proof is detailed in Appendix C-B. □

B. Symbol error rate evaluation

Using the ML criterion in Lemma 2, the correct detection zone $\mathcal{D}$ around a symbol s_0 is the Voronoï region centered around s_0 such that

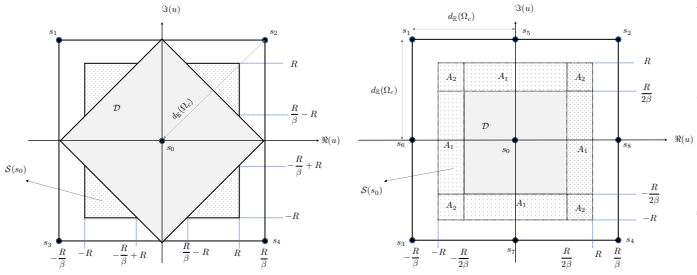
$$\mathcal{D}(\mathcal{L}) = \mathcal{V}(s_0) = \{v \in \mathbb{C} : |s_0 - v| \leq |s - v|, \forall s \in \mathcal{L}\} \tag{25}$$

with $\mathcal{L} = \Lambda_k$ at Bob and $\mathcal{L} = \Omega_c$ at Eve. The bounds of the detection region depend on the scaled minimal Euclidean

distance where $d_{\mathbb{E}}(\Lambda_k) = \frac{2R}{\beta}$ and is equal to $d_{\mathbb{E}}(\Omega_c) = \frac{2R}{2^{\ell/2}\beta}$. The symbol error probability is,

$$\mathbb{P}_e = \text{Prob}\{u_z = (u + h^{-1}z) \notin \mathcal{D}(\mathcal{L})\}, \tag{26}$$

where $\mathcal{D}(\mathcal{L})$ is the detection zone specified in Figure 6 and u_z is the random noise with coordinates in the rotated $\frac{\pi}{4}$- system for $\ell = 1$ or the Cartesian system for $\ell = 2$, having as pdf distribution detailed in Lemma 1. In the high SNR regime, the



(a) Eve with $\ell = 1$, $\mathcal{S} \cap \mathcal{D} \neq \mathcal{S}$ (b) Eve with $\ell = 2$, $\mathcal{D} \subseteq \mathcal{S}$

Fig. 6: Error detection zone $\mathcal{D}$ is in gray and the uniform noise domain space $\mathcal{S}$ is filled with a dot pattern

average BER can be deduced from the most dominant error event computed in (26) as,

$$\text{BER}^{(b),(e)}(\text{SNR}) = \frac{\bar{d}_{\mathbb{H}}^{(b),(e)}}{q-\ell}\mathbb{P}_e^{(b),(e)}(\text{SNR}), \tag{27}$$

with $\bar{d}_{\mathbb{H}}^{(b)}$ (resp. $\bar{d}_{\mathbb{H}}^{(e)}$) being the average Hamming distance in Λ_k (resp. Ω_c) that are summarized in Table I.

1) Error rate evaluation at Eve: At the eavesdropper, the SER is computed from (26) where the detection zone with one-bit partitioning is such that,

$$\mathcal{D}_1(\Omega_c) = \big\{u_z \in \mathbb{C} : |\Re(u_z)| < \frac{R}{\beta}; |\Re(u_z)| + |\Im(u_z)| < \frac{R}{\beta}\big\},$$

and for two-bits partitioning,

$$\mathcal{D}_2(\Omega_c) = \big\{u_z \in \mathbb{C} : |\Re(u_z)| < \frac{R}{2^{\ell/2}\beta}; |\Im(u_z)| < \frac{R}{2^{\ell/2}\beta}\big\}.$$

We can notice from Figure 6a, that if the detection zone $\mathcal{D}_1(\Omega_c) \cap \mathcal{S} = \mathcal{S}$, the symbol error probability becomes negligible in the high SNR regime. However, $\mathcal{D}_1(\Omega_c) \cap \mathcal{S} \neq \mathcal{S}$, requires that $\frac{1}{2} \leq \beta \leq 1$. Similarly, $\mathcal{D}_2(\Omega_c) \cap \mathcal{S} \neq \mathcal{S}$ if $\frac{1}{2} \leq \beta \leq 1$. The expansion of these SER expressions shows that in the high SNR regime, the SER achieves a constant high SER floor as detailed in Theorem 2.

Theorem 2 (eavesdropper error rate)**.** *For $\frac{1}{2} \leq \beta \leq 1$, the SER at the eavesdropper, for a noisy IPM considering 2^q-QAM constellation ($q \neq 2$) achieves a constant error floor: For the one-bit partitioning ($\ell = 1$):*

$$\mathbb{P}_e^{(e,1)} \approx 2(1 - 2^{-q/2})\left(1 - \frac{1}{2\beta}\right)^2 + o(\text{SNR}^0). \tag{28}$$

For the two-bit partitioning ($\ell = 2$):

$$\mathbb{P}_e^{(e,2)} \approx (1 - 2^{-q})\Big(1 - \frac{1}{2\beta}\Big)\left(1 + \frac{1 - 2^{-q/2}}{1 + 2^{-q/2}}\frac{1}{2\beta}\right) + o(\text{SNR}^0), \tag{29}$$

which is approximately equal to $\mathbb{P}_e^{(e,2)} \approx 1 - \frac{1}{4\beta^2}$ for high modulation order. A correction term should be added to the SER when attempting to decode two symbols carrying the same information binary sequence, as, $\mathbb{P}_{e,c}^{(e,2)} = \mathbb{P}_e^{(e,2)} - 2^{-q}\left(1 - \frac{1}{2\beta}\right)^2$. For the case of QPSK constellation with one-bit partitioning, $\mathbb{P}_e^{(e,1)} \approx \left(1 - \frac{1}{2\beta}\right)^2$.

Proof. The proof is provided in Appendix D-A. □

2) Error rate evaluation at Bob: At the legitimate receiver, the error rate is computed from (26) where

$$\mathcal{D}^{(\ell=1,2)}(\Lambda_k) = \big\{u_z \in \mathbb{C} : |\Re(u_z)| < \frac{R}{\beta} \text{ and } |\Im(u_z)| < \frac{R}{\beta}\big\}.$$

The expansion of this expression is detailed in Theorem 3 given $|h|$. The average error rate considering Rayleigh fading channel distribution as well as its asymptotic behavior are computed in Corollaries 3.1 and 3.2.

Theorem 3 (General case)**.** *Let $\hat{s}$ be the decoded symbol at the receiver side and s_0 being the transmitted one. Considering the general noisy-IPM, the symbol error probability at Bob is,*

$$\mathbb{P}_e^{(b)}(\text{SNR}^{(b)}) \approx \frac{\bar{N}_a^{(b)}}{2^{\ell/2}\beta}\mathbb{E}_h\Big[\mathbb{P}_{e,1}^{(b)}(\text{SNR}^{(b)}) + \mathbb{P}_{e,2}^{(b)}(\text{SNR}^{(b)})\Big], \tag{30}$$

where

$$\mathbb{P}_{e,1}^{(b)} = 2\eta_p Q\big(\eta_p\sqrt{\text{SNR}_h^{(b)}}\big) - 2\eta_m Q\big(\eta_m\sqrt{\text{SNR}_h^{(b)}}\big), \tag{31}$$

$$\mathbb{P}_{e,2}^{(b)} = \sqrt{\frac{2}{\pi\,\text{SNR}_h^{(b)}}}\left[\exp\left(\frac{-\eta_m^2}{2}\,\text{SNR}_h^{(b)}\right) - \exp\left(\frac{-\eta_p^2}{2}\,\text{SNR}_h^{(b)}\right)\right], \tag{32}$$

with $\text{SNR}_h = \frac{\theta\,\text{SNR}_b\,|h^{(b)}|^2}{E_s}$, $\eta_m = 2^{\ell/2}(1-\beta)$, $\eta_p = 2^{\ell/2}(1+\beta)$ and $\bar{N}_a^{(b)} = \frac{1}{4}\bar{N}^{(b)}$ with $\bar{N}^{(b)}$ defined in (7) and (8).

Proof. The proof is provided in Appendix D-B. □

Corollary 3.1 (Average SER with Rayleigh fading distribution)**.** *For noisy IPM case, the average symbol error probability considering the Rayleigh distribution of $|h|$ is,*

$$\mathbb{P}_e^{(b)}(\text{SNR}^{(b)}) \approx \frac{\bar{N}_a^{(b)}}{2^{\ell/2}\beta}\Big[\bar{\mathbb{P}}_{e,1}(\text{SNR}^{(b)}) + \bar{\mathbb{P}}_{e,2}(\text{SNR}^{(b)})\Big], \tag{33}$$

where

$$\bar{\mathbb{P}}_{e,1}^{(b)} = \eta_p - \eta_m + \frac{\eta_m^2\sqrt{\text{SNR}_u^{(b)}}}{\sqrt{\eta_m^2\,\text{SNR}_u^{(b)} + 1}} - \frac{\eta_p^2\sqrt{\text{SNR}_u^{(b)}}}{\sqrt{\eta_p^2\,\text{SNR}_u^{(b)} + 1}}, \tag{34}$$

$$\bar{\mathbb{P}}_{e,2}^{(b)} = \frac{1}{\sqrt{\text{SNR}_u}}\left(\frac{1}{\sqrt{\eta_m^2\,\text{SNR}_u^{(b)} + 1}} - \frac{1}{\sqrt{\eta_p^2\,\text{SNR}_u^{(b)} + 1}}\right) \tag{35}$$

with $\text{SNR}_u^{(b)} = \frac{\theta}{E_s}\,\text{SNR}^{(b)}$.

Proof. The proof is detailed in Appendix D-C. □

Corollary 3.2 (Asymptotic behavior for noisy IPM)**.** *In the high SNR regime, the symbol error probability behavior at the legitimate receiver is:*

1) *Partial-noisy Voronoï region where* $0 \leq \beta < 1$,

$$\mathbb{P}_e^{(b)}(\mathrm{SNR}^{(b)}) \approx \frac{\bar{N}_a^{(b)}}{2^{\ell}(1-\beta^2)} \frac{\theta}{E_s} \frac{1}{\mathrm{SNR}^{(b)}} + o(\mathrm{SNR}^{-1}). \tag{36}$$

2) *Full-noisy Voronoï region* $\beta = 1$,

$$\mathbb{P}_e^{(b)}(\mathrm{SNR}^{(b)}) \approx \frac{\bar{N}_a^{(b)}}{2^{\ell/2}} \frac{\theta}{E_s} \frac{1}{\sqrt{\mathrm{SNR}^{(b)}}} + o(\mathrm{SNR}^{-1}); \tag{37}$$

Proof. The proof is provided in Appendix D-D. □

C. Vulnerabilities and countermeasures

In this subsection, we consider different types of attacks that can be exploited by the eavesdropper to compromise the security of IPM scheme.

1) Reuse of the same common seed: In non-dynamic environments, there is a non-zero probability to get, based on quantized wireless channel estimation, identical common seeds for two neighboring legitimate receivers. This situation arises when the transmitter communicates with two neighboring users within a period that is lower than the coherence time. By tracking the position of users, the eavesdropper can make use of the same index reuse to perform joint decoding in $\Lambda_{\boldsymbol{k}} \times \Lambda_{\boldsymbol{k}} \subset \Omega_c^2$ for all values of $\boldsymbol{k}$. As a result of this joint decoding in the subset $\Lambda_{\boldsymbol{k}} \times \Lambda_{\boldsymbol{k}}$ instead of Ω_c^2, the BER at the eavesdropper is significantly enhanced. The common seed reuse weakens the security of the encryption and compromise the communication security. To overcome this problem, the transmitter needs to save within the coherence time the values of the common seed used to initialize the PRNG. If a reuse of the same common seed is detected, the transmitter indicates to the receiver to change the default precision parameter of the congruential PRNG from $p = 12$ to another random integer value (Line 1 in Algorithm 1). This modification ensures that the legitimate receivers' binary index sequences are distinct.

2) Highly correlated wireless legitimate and eavesdropper paths: Most of literature work on physical layer key generation assumes that the distance between Eve and Bob is higher than half of the wavelength. This assumption guarantees that the wireless paths are uncorrelated and that the common seed quantized on 128 bits cannot be predicted at the eavesdropper. However, in the case that Eve is situated at a distance that is less than half of the wavelength to Bob, the correlation between their wireless channels will create a risk of Eve predicting the common seed. To avoid this worst case scenario and to limit the vulnerability window, a regular update for the physical layer key should be performed at intervals that are higher than the coherence time.

3) Attack with spatially distributed and coorperative eavesdropper: When different spatially distributed eavesdroppers cooperate to intercept the signal, the noisy signal is decoded on an equivalent Single Input Multiple Output channel. In the high SNR regime, we have shown in Theorem 2 that the error probability at the eavesdropper is independent of the SNR. The receiver diversity does not enhance the eavesdropper error rate.

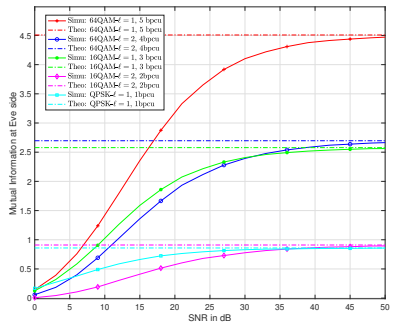
VI. Numerical results

In this section, we numerically evaluate the performance of the noisy IPM in terms of secrecy rate and error rate, as well as its robustness against attacks.

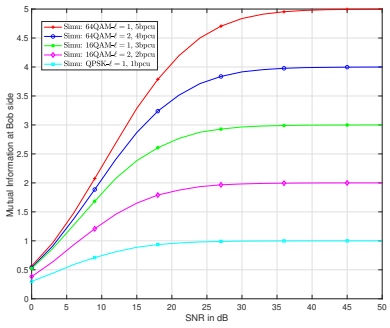
A. Secrecy performances

Figures 7a and 7b compare the mutual information of the IPM scheme for Bob and Eve considering three modulation schemes 64-QAM, 16-QAM with one and two bits index length and a QPSK with a one-length index. In the high SNR regime, Bob's mutual information in Figure 7b converges to $(q - \ell)$ bits per channel use (bpcu). However, the mutual information of Eve in Figure 7a is degraded compared to Bob and it reaches a plateau value that is significantly lower than $(q - \ell)$ bpcu in the high SNR regime. We can notice that the theoretical asymptotic values computed in Corollary 1.1 and illustrated in dot-dash lines converge towards the simulated ones. Knowing the dynamic index, Bob is able to decode its own information considering only the indexed partition with distant neighboring symbols. However, Eve has to consider the whole constellation Ω_c and to deal with the confusing uniform AN that adds random perturbation to the symbols in an area that exceeds their Voronoï region. This noise will not affect the legitimate receiver as the random uniform AN lies inside the Voronoï region of the symbols belonging to a single partition. Figures 7c and 7d compare the SER at Eve and Bob. Figure 7c shows that for all the spectral efficiencies, the SER at Eve achieve plateau values that converge to the theoretical ones computed in Theorem 2. We can also see that the SER at Eve with two-bits partitioning is higher than the one-bit partitioning. This is a consequence that the error occurs almost surely when the received noisy IPM symbol is situated at the intersection of random uniform AN region and outside the Voronoï region around a symbol. This region is larger with two-bits partitioning than with one-bit partitioning. At Bob, the SER decays in function of SNR, and the theoretical values in Corollary 3.1 as well as the asymptotical ones in Corollary 3.2 converge to the simulated ones.

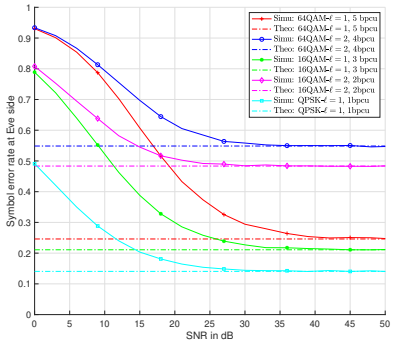
Figures 7e and 7f compare the SER at Eve and Bob considering different values of β with $\mathrm{SNR} = 20$ dB. For all the spectral efficiencies, the performance of Eve in terms of SER and secrecy rate are degraded when increasing the value of β. The injected noise becomes more powerful when beta increases and the domain space of the random uniform noise becomes larger. This will increase the confusion at the eavesdropper and will increase the SER and the secrecy rate. The partitioning with two bits has better performances than the one bit partitioning. The increases of β degrades the performance of Eve but also degrades the ones of Bob. However, the SER remains low enough in the ranges of 10^{-3} to 10^{-4} at an SNR of 20 dB. A trade-off between the degradation of the quality of the transmission at Eve and the correct detection at Bob should be found by adjusting the value of β and the spectral efficiency.



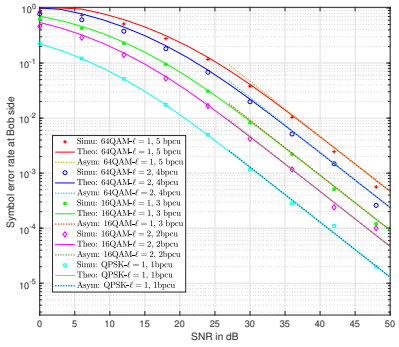
(a) Eve: Mutual Information ($\beta = 0.8$)



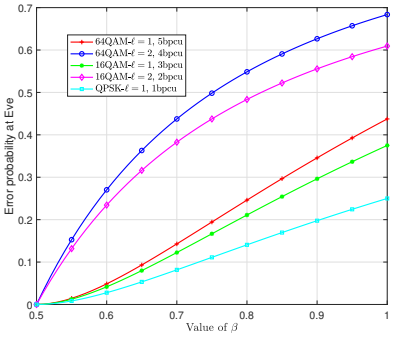
(b) Bob: Mutual Information ($\beta = 0.8$)



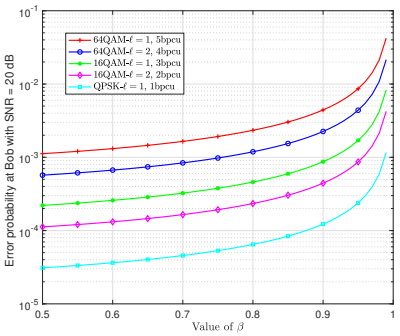
(c) SER at Eve ($\beta = 0.8$)



(d) SER at Bob ($\beta = 0.8$)

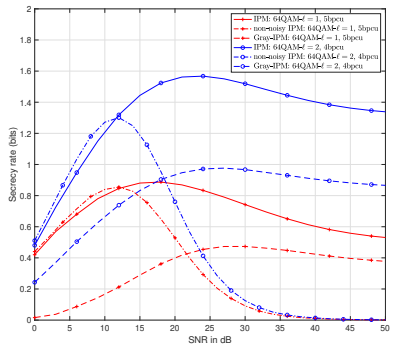


(e) Variation of Eve SER with β ($\text{SNR}_e > 20$ dB)

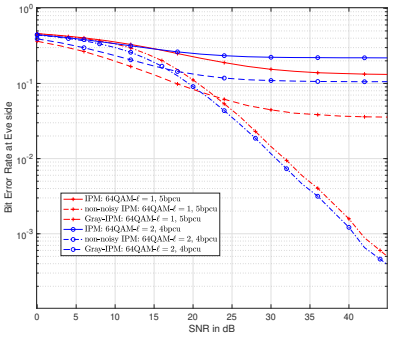


(f) Variation of Bob SER with β ($\text{SNR}_b = 20$ dB)

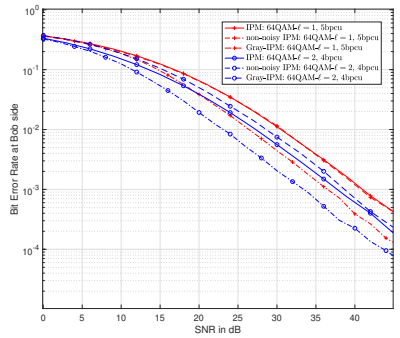
Fig. 7: SER and mutual information at Eve and Bob



(a) Secrecy rate with 64QAM



(b) BER at Eve



(c) BER at Bob

Fig. 8: Comparison of IPM ($\beta = 0.8$), IPM with Gray labeling ($\beta = 0.8$) and noiseless IPM

To compare the efficiency in terms of BER and secrecy rate of our proposed IPM scheme, we consider two other schemes:

- Non noisy IPM with $\beta = 0$. In this case, the injected random uniform noise is null.
- IPM with Gray labeling: we can notice that the Gray labeling of the QAM constellation symbols with a binary label $b_0 b_1 \dots b_{n-1}$ partitions the QAM constellation into two sets by considering that $b_0 = b_1 \oplus \dots b_{n-1}$ when the index is equal zero, and $b_0 = 1 \oplus (b_1 \oplus \dots b_{n-1})$ when the index is equal to one.The four set partitioning case is obtained by considering that, $b_0 = b_1 \oplus \dots b_{\frac{q}{2}-1}$ and $b_q = b_{\frac{q}{2}} \oplus \dots b_{q-1}$ $b_0 = 1 \oplus (b_1 \oplus \dots b_{\frac{q}{2}-1})$ and $b_q = b_{\frac{q}{2}} \oplus \dots b_{q-1}$ if the index is equal to 01, $b_0 = b_1 \oplus \dots b_{\frac{q}{2}-1}$ and $b_q = 1 \oplus (b_{\frac{q}{2}} \oplus \dots b_{q-1})$ if the index is equal to 10, and $b_0 = 1 \oplus (b_1 \oplus \dots b_{\frac{q}{2}-1})$ and $b_q = 1 \oplus (b_{\frac{q}{2}} \oplus \dots b_{q-1})$ if the index is equal to 11.

Table II compares the Hamming distribution of the Gray mapping and our proposed cross-labeling for a 64QAM constellation with one or two bits partitioning. At Eve, the probability to get a zero Hamming distance between two neighboring symbol

TABLE II: Hamming distance distribution

			0	1	2	3	4
$\ell=1$	Eve	Cross	0	0.07	0.36	0.43	0.14
		Gray	0.28	0.72	0	0	0
	Bob	Cross	0	0.82	0	0.18	0
		Gray	0	0.57	0.43	0	0
$\ell=2$	Eve	Cross	0	0.57	0.43	0	0
		Gray	0.36	0.64	0	0	0
	Bob	Cross	0	1	0	0	0
		Gray	0	0.64	0.36	0	0

is non-zero compared with our cross-labeling. This means that the injected random uniform noise will not always degrade the BER at Eve. Indeed, the Gray mapping degrades slightly the BER at Bob as the average Hamming distance with the Gray mapping is higher than the cross-labeling.

Figure 8a compares the secrecy rate of the 64-QAM constellation considering one or two bits partitioning, with the noiseless IPM case and the IPM with Gray labeling. For noiseless IPM, the average mutual information of Eve converges to the maximal spectral efficiency $(q-\ell)$, and the secrecy rate converges to zero at high SNR. Compared to the Gray-labeling, the cross-labeling maximizes the secrecy rate as observed in Figure 8a. The same behavior of the Gray-labeling versus the cross-labeling is also observed in the BER in Figure 8. For the noiseless IPM, the BER at Eve in Figure 8b decays with SNR with a small loss in coding gain compared to Bob. At Bob in Figure 8c, the BER is slightly degraded by the random uniform noise compared with the noiseless case.

B. Secrecy robustness

As explained in Subsection V-C, the error probability at the eavesdropper decreases with the reuse of common seed to initialize the logistic map. However, the error rate at the eavesdropper remains unchanged when multiple distributed eavesdroppers cooperate to decode the signal. Table III compares the SER at the eavesdropper without reuse of the common and with two reuse of the common seed. We also compute the SER considering 4 cooperative eavesdroppers. As mentioned, the common seed reuse problem can be mitigated by changing the parameter of the congruential PRNG. By changing in Algorithm 1 the parameter p from 12 to 14, 50% of the bits generated in the new sequence are different than the previous one.

TABLE III: SER at the eavesdropper (16QAM ℓ = 2)

SNR	25	30	35	40
Unique index	0.6465	0.6538	0.6446	0.6354
Reused index	0.2856	0.2939	0.2880	0.2836
Cooperative	0.6486	0.6541	0.6453	0.6353

VII. Conclusion

In this paper, we proposed a new PLS scheme, referred noisy and dynamic IPM to secure wireless communication against eavesdropping in a non-degraded wiretap channel. The IPM scheme relies on three main components: a dynamic index generator that selects the secret partition at each time, a QAM cross-labelling and a random uniform noise injection. Our analytical and numerical results show that the IPM creates an error floor on the eavesdropping link while maintaining transmission quality on the legitimate link. Compared to a classical modulation, the IPM does not increase the computational complexity at the transmitter or at the receiver side. However, the regular updates of physical layer key generation exhibit additional complexity at all the legitimate entities. Indeed, perfect synchronization is required to ensure that the same partition index is used at the transmitter and the receiver sides. The IPM scheme is compliant with wireless technologies based on QAM constellation such as the IEEE 802.11p used in Intelligent Transportation Systems (ITS). In the context of vehicular communication, eavesdropping compromises the privacy and the anonymity of sensitive information such as vehicle location, travel pattern, personal information of travelers. The power of artificial noise is adjusted using the parameter β to induce confusion at the eavesdropper, depending on the information's sensitivity [1].

Appendix A
Proof of Lemma 1

The proof of this Lemma is obtained from the convolution between Gaussian distribution and uniform one. Note that, for the index of length 1, the square region inside the Voronoï region is rotated with an angle of $\pi/4$. As the rotation does not change the Gaussian distribution of the complex random noise, in both cases of 1-bit or 2-bits of index length, the random uniform noise u varies in a square region $\mathcal{S}$ defined in the $\pi/4$-rotated coordinate system for $\ell=1$ and in the Cartesian one for $\ell=2$.

Appendix B
proof of Lemma 2

The variation of $\omega(y|s_0,h)$ as a function of $\nu=|u_z|$ is deduced from the derivative of $\omega(.)$ with respect to ν,

$$\frac{\partial\omega}{\partial\nu}=\frac{\partial\omega}{\partial u_{z,r}}\frac{\partial u_{z,r}}{\partial\nu}+\frac{\partial\omega}{\partial u_{z,i}}\frac{\partial u_{z,i}}{\partial\nu}.$$

By computing the partial derivatives,

$$\begin{aligned}\frac{\partial\omega}{\partial u_{z,r}} &= \frac{p_i}{4R^2}\Big(e^{-\frac{(R+u_{z,r})^2}{\sigma_h^2}}-e^{-\frac{(R-u_{z,r})^2}{\sigma_h^2}}\Big),\\ p_i &= \Phi\left(\frac{R-u_{z,i}}{\sigma_h}\right)-\Phi\left(-\frac{R+u_{z,i}}{\sigma_h}\right),\\ \frac{\partial u_{z,r}}{\partial\nu} &= \frac{\nu}{u_{z,r}}.\end{aligned}$$

Note first that p_i is the probability that a Gaussian value to be bounded by two values and is then $0\le p_i\le 1$. If $u_{z,r}>0$, $\frac{\partial\omega}{\partial u_{z,r}}<0$ and $\frac{\partial u_{z,r}}{\partial\nu}>0$. If $u_{z,r}>0$, then, $\frac{\partial\omega}{\partial u_{z,r}}>0$ and $\frac{\partial u_{z,r}}{\partial\nu}<0$. This means that in both case cases $\frac{\partial\omega}{\partial u_{z,r}}\frac{\partial u_{z,r}}{\partial\nu}<0$. In a similar manner, $\frac{\partial\omega}{\partial u_{z,i}}\frac{\partial u_{z,i}}{\partial\nu}$ is also negative. Consequently, $\frac{\partial\omega}{\partial\nu}<0$. Maximizing the function

$\omega(y|s_0,h)$ is then equivalent to minimize ν. At the legitimate receiver, the index k is assumed to be perfectly known. The ML estimation is then performed within the alphabet Λ_k. At the eavesdropper, the estimated symbol resulting from the MAP decoding is $\hat{s} = \arg\min_k \min_{s\in\Lambda_k} |y - \sqrt{\theta P}hs|^2$. This is equivalent to search for the minimal distance in Ω_c.

APPENDIX C
SECRECY RATE

A. Proof of Theorem 1

The average mutual information between the transmitted information signal at Alice and the received one $y^{(b)}$ at Bob knowing the dynamic index $\boldsymbol{k}$ is,

$$\mathrm{I}_b(\psi(\boldsymbol{b}), y^{(b)}|\boldsymbol{k}) = \mathbb{E}\big[\mathrm{H}(y^{(b)}|\boldsymbol{k}) - \mathrm{H}(y^{(b)}|s_0,\boldsymbol{k})\big], \quad (38)$$

where s_0 is the normalized corresponding symbol in Λ_k and $\mathrm{H}(.)$ is the entropy of a random variable, such that,

$$\mathrm{H}(y^{(b)}|h^{(b)},\boldsymbol{k}) = -\log_2 f(y^{(b)}|h^{(b)},\boldsymbol{k}), \quad (39)$$
$$\mathrm{H}(y^{(b)}|s_0,h^{(b)}) = -\log_2 f(y^{(b)}|s_0,h^{(b)},\boldsymbol{k}). \quad (40)$$

The conditional probability in (39) is computed by marginalizing over all the possibilities of $s_0 \in \Lambda_k$,

$$f(y^{(b)}|h^{(b)},\boldsymbol{k}) = \frac{1}{2^{q-\ell}} \sum_{s_0\in\Lambda_k} f\big(y^{(b)}|s_0,h^{(b)}\big).$$

Combining (38) and (41), the average mutual information in (20) is deduced. Unlike Bob, Eve is not aware of the value of the key index. The Eve's mutual information is,

$$\mathrm{I}_e(\psi(\boldsymbol{b}), y^{(e)}) = \mathbb{E}\big[\mathrm{H}(y^{(e)}) - \mathrm{H}(y^{(e)}|\psi(\boldsymbol{b})\big], \quad (41)$$
$$\mathrm{H}(y^{(e)}|h^{(e)}) = -\log_2 f(y^{(e)}|h^{(e)}), \quad (42)$$
$$\mathrm{H}(y^{(e)}|\psi(\boldsymbol{b}),h^{(e)}) = -\log_2 f(y^{(e)}|\psi(\boldsymbol{b}),h^{(e)}). \quad (43)$$

At Eve, $\boldsymbol{k}$ is not known and the probability in (42) is the marginalization over all the values of $s_0 \in \Omega_c$,

$$f(y^{(e)}|h^{(e)}) = \frac{1}{2^q} \sum_{s_0\in\Omega_c} f\big(y^{(e)}|s_0,h^{(e)}\big).$$

Indeed, the information bit vector $\boldsymbol{b}$ has multiple image in Ω_c, and the conditional probability in (43) is computed,

$$f(y^{(e)}|\psi(\boldsymbol{b}),h^{(e)}) = \frac{1}{2^\ell} \sum_{\boldsymbol{k}} f(y^{(e)}|\psi(\boldsymbol{b}|\boldsymbol{k}),h^{(e)})$$

By combining (41), (44) and (44), the average mutual information in (21) is deduced.

B. Proof of Corollary 1.1

Let s_0 be the transmitted symbol and $y^{(b)}$ (resp. $y^{(e)}$) the noisy received signal at Bob (resp. Eve) with $\sigma_h \to 0$. The mutual information in Theorem 1 depends on $\omega(y|s,h)$ given in Lemma 1. For $\sigma_h \to 0$, the value of u_z in Lemma 1 is

$$u_z = \sqrt{\theta P}(s_0 - s) + u. \quad (44)$$

The variation set of s is provided in Theorem 1 where $s \in \Lambda_k$ at Bob and $s \in \Omega_c$ at Eve. The limit of $\omega(y|s,h)$ is,

$$\lim_{\sigma_h\to 0} \omega(y|s,h) = \frac{1}{|\mathcal{S}|}\mathbb{1}(u_z \in \mathcal{S}). \quad (45)$$

At the legitimate receiver, the computation of the mutual information $\mathrm{I}_b(\psi(\boldsymbol{b}), y^{(b)}|\boldsymbol{k})$ requires to compute:

$$\sum_{s\in\Lambda_k} \frac{\omega(y^{(b)}|s,h^{(b)})}{\omega(y^{(b)}|s_0,h^{(b)})} = 1 + \sum_{s\neq s_0 : s\in\Lambda_k} \mathbb{1}(u_z \in \mathcal{S}).$$

Given a partition Λ_k and $\forall s \neq s_0 \in \Lambda_k$, the set of potential symbols s that ensure that $u_z \in \mathcal{S}$ is empty as the closest points to s_0 are $s_0 - s = \pm 2^{\ell/2} d_{\min}$ or $s_0 - s = \pm(2^{\ell/2} d_{\min})1i$ with $2^{\ell/2} d_{\min} \geq \beta 2^{\ell/2} d_{\min}$. Consequently, $\sum_{s\neq s_0 : s\in\Lambda_k} \mathbb{1}(u_z \in \mathcal{S}) = 0$. The mutual information at the legitimate receiver is then $\lim_{\sigma_h\to 0} \mathrm{I}_b(\psi(\boldsymbol{b}), y^{(b)}|\boldsymbol{k}) \to (q-\ell)$.

At the eavesdropper receiver, the computation of the mutual information requires to compute:

$$F = \frac{\sum_{s\in\Omega_c} \omega(y^{(e)}|s,h^{(e)})}{\omega(y^{(e)}|s_0,h^{(e)}) + \sum_{k:\psi(\boldsymbol{b}|\boldsymbol{k})\neq s_0} \omega(y^{(e)}|\psi(\boldsymbol{b}|\boldsymbol{k}),h^{(e)})}.$$

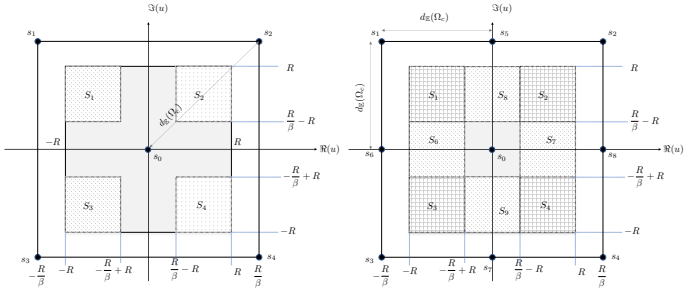
Note first that due to (45)

$$\sum_{\boldsymbol{k}:\psi(\boldsymbol{b}|\boldsymbol{k})\neq s_0} \omega(y^{(e)}|\psi(\boldsymbol{b}|\boldsymbol{k}),h^{(e)}) = \frac{1}{|\mathcal{S}|} \sum_{\boldsymbol{k}:\psi(\boldsymbol{b}|\boldsymbol{k})\neq s_0} \mathbb{1}(u_{z,\boldsymbol{k}} \in \mathcal{S})$$

with $u_{z,\boldsymbol{k}} = \sqrt{\theta P}(\psi(\boldsymbol{b}|\boldsymbol{k}) - s_0) + u$. The bit labeling in Subsection III-B guarantees that $\sqrt{\theta P}|(\psi(\boldsymbol{b}|\boldsymbol{k}) - s_0)| > 2R$ for all cases except some particular cases that will be separately studied in the following. In all the other cases, $\sum_{k:\psi(\boldsymbol{b}|\boldsymbol{k})\neq s_0} \omega(y^{(e)}|\psi(\boldsymbol{b}|\boldsymbol{k}),h^{(e)}) = 0$ and

$$F = \sum_{s\in\Omega_c} \frac{\omega(y^{(e)}|s,h^{(e)})}{\omega(y^{(e)}|s_0,h^{(e)})} = 1 + \sum_{s\neq s_0 : s\in\Omega_c} \mathbb{1}(u_z \in \mathcal{S}). \quad (46)$$

As in the previous case, we need to identify the set $\mathcal{N}_s$ of feasible symbols $s \in \Omega_c$ ensuring $u_z \in \mathcal{S}$. If $0 \leq 2\beta < 1$, then $\mathcal{N}_s = \emptyset$ as the distance between two symbols is at least $d_{\min}$. $\mathcal{N}_s$ is a non-empty set if $2\beta > 1$.



(a) $\ell = 1$ (b) $\ell = 2$

Fig. 9: Confusion-regions

1) One-bit partitioning: For $\ell = 1$, the set of $s \in \Omega_c$ is $\mathcal{N}_s = \{s_0 + d_{\min} 2^{-\frac{1}{2}}(\pm 1 \pm 1i)\}$. For each $s \in \mathcal{N}_s$, we need to determine the area of variation of u. The corresponding regions are disjoint and are illustrated in Figure 9a and have identical area, $|S_i| = \left(2R - \frac{R}{\beta}\right)^2, 1 \leq i \leq 4$. The value of F in (46) is then equal to 1 or 2, such that,

$$F = \begin{cases} 1 & u \notin \bigcup_{s\in\mathcal{N}_s} S_i, \\ 2 & u \in \bigcup_{s\in\mathcal{N}_s} S_i, \end{cases}$$

where $\bigcup_{s\in\mathcal{N}_s} S_i$ depends on the number of neighboring symbols around s_0, *i.e.*

$$\text{Prob}\left\{u \in \cup_{s\in\mathcal{N}_s} S_i\right\} = \mathbb{E}[|\mathcal{N}(s_0)|]\left(1-\frac{1}{2\beta}\right)^2 \quad (47)$$

where $\bar{N}^{(e)} = \mathbb{E}[|\mathcal{N}_s(s_0)|]$ is the average number of neighbors around a point in Ω_c given in (9). It follows that,

$$\mathbb{E}(\log_2(F)) \;=\; \bar{N}^{(e)}\left(1-\frac{1}{2\beta}\right)^2,$$

For the QPSK partitioned with one bit, the symbols around the origin, map the same information bit 0 or 1. This means that, $\sqrt{\theta P}|\psi(0|0)-\psi(0|1)| < 2R$. In this case, $\sum_{k:\psi(\boldsymbol{b}|\boldsymbol{k})}\omega(y^{(e)}|\psi(\boldsymbol{b}|\boldsymbol{k}),h^{(e)}) = \frac{2}{|\mathcal{S}|}$. By repeating similar step as before, $\mathbb{E}[\log_2(F)] = \left(1-\frac{1}{2\beta}\right)^2$.

2) Two-bits partitioning: For $\ell = 2$, the set of $s \in \Omega_c$ is $\mathcal{N}_s = \{\pm d_{\min}, \pm d_{\min}\times 1i, d_{\min}(\pm 1 \pm 1i)\}$. In Figure 9a, the values of $s \in \mathcal{N}_s$ for which the conditions S_1 are satisfied are $s_0 + d_{\min}, s_0 + d_{\min}(1-1i), s_0 - d_{\min}1i$. In this case, $\sum_{s\neq s_0: s\in\Omega_c}\mathbb{1}(u_z \in \mathcal{S}) = 3$ if the three neighbors are $\in \Omega_c$. In Figure 9b, the values of $s \in \mathcal{N}_s$ for which the conditions S_6 is satisfied for $s = s_0 + d_{\min}$. This means that $\sum_{s\neq s_0: s\in\Omega_c}\mathbb{1}(u_z \in \mathcal{S}) = 1$. The value of F depends on the cardinality of $\mathcal{N}_s$ the set of neighbors around s_0:

1) Case of $|\mathcal{N}_s| = 2$ with $\text{Prob}\{|\mathcal{N}_s| = 2\} = \frac{1}{2^{q-2}}$ (consider the right-lower quadrant) :

$$F = \begin{cases} 4 & u \in S_4 \\ 2 & u \in (S_3 \cup S_9) \cup (S_2 \cup S_7) \\ 1 & \text{otherwise} \end{cases}$$

2) Case of $|\mathcal{N}_s| = 3$ with probability $\text{Prob}\{|\mathcal{N}_s| = 3\} = \frac{2(2^{\frac{q-2}{2}}-1)}{2^{q-2}}$ (consider the lower half in Figure 9b):

$$F = \begin{cases} 4 & u \in (S_3 \cup S_4) \\ 2 & u \in (S_1 \cup S_6) \cup S_9 \cup (S_2 \cup S_7) \\ 1 & \text{otherwise} \end{cases}$$

3) Case of $|\mathcal{N}_s| = 4$ with $\text{Prob}\{|\mathcal{N}_s| = 4\} = \frac{(2^{\frac{q-2}{2}}-1)^2}{2^{q-2}}$:

$$F = \begin{cases} 4 & u \in S_1 \cup S_2 \cup S_3 \cup S_4 \\ 2 & u \in S_5 \cup S_6 \cup S_7 \cup S_8 \\ 1 & \text{otherwise} \end{cases}$$

By replacing the values of the disjoint surfaces by their values as, $|S_1| = |S_2| = |S_3| = |S_4| = 4R^2(1-\frac{1}{2\beta})^2$ and $|S_6| = |S_7| = |S_8| = |S_9| = 4R^2(\frac{1}{\beta}-1)(1-\frac{1}{2\beta})$ we can deduce,

$$\mathbb{E}[\log_2(F)] = \bar{N}^{(e)}(1-\frac{1}{2\beta}). \quad (48)$$

A correction term should be added to take into account the bit labeling, as there exist in the constellation 4 symbols in Ω_c around the origin $\pm 1 \pm 1i$ for which $\sqrt{\theta P}|(\psi(\boldsymbol{b}|\boldsymbol{k}) - s_0)| < 2R$. This can be observed for the 16QAM constellation in Figure 3b where $\sqrt{\theta P}|(\psi(10|11) - \psi(10|00))| < 2R$ and also $\sqrt{\theta P}|(\psi(01|10) - \psi(01|01))| < 2R$. This is also the case for a 64-QAM where $\sqrt{\theta P}|(\psi(1101|11) - \psi(1101|00))| < 2R$ and also $\sqrt{\theta P}|(\psi(0111|10) - \psi(0111|01))| < 2R$. In this case, $\sum_{k:\psi(\boldsymbol{b}|\boldsymbol{k})}\omega(y^{(e)}|\psi(\boldsymbol{b}|\boldsymbol{k}),h^{(e)}) = \frac{2}{|\mathcal{S}|}$ and $F = \frac{1}{2}\sum_{s\neq s_0: s\in\Omega_c}\mathbb{1}(u_z \in \mathcal{S})$ on a single quadrant of Figure 9b. For this particular constellation symbol,

$$F = \begin{cases} 4 & u \in S_1 \cup S_2 \cup S_3 \\ 2 & u \in S_5 \cup S_6 \cup S_7 \cup S_8 \cup S_4 \\ 1 & \text{otherwise} \end{cases}$$

When averaging over all constellation points in (48), a correction term should be added as,

$$\mathbb{E}[\log_2(F)] = \bar{N}^{(e)}\left(1-\frac{1}{2\beta}\right) - \frac{1}{2^{q-2}}\left(1-\frac{1}{2\beta}\right)^2.$$

APPENDIX D
ERROR RATE EVALUATION

A. Proof of Theorem 2

The SER at the eavesdropper can be written as,

$$\text{Prob}\{u_z \notin \mathcal{D}\} = \text{Prob}\{u_z \in \mathcal{S}\cap\bar{\mathcal{D}}\} + \text{Prob}\{u_z \in \bar{\mathcal{S}}\cap\bar{\mathcal{D}}\}.$$

In the high SNR regime, the random uniform noise is dominant and the SER reduces to,

$$\lim_{\sigma\to 0}\text{Prob}\{u_z \notin \mathcal{D}\} = \text{Prob}\{u_z \in \mathcal{S}\cap\bar{\mathcal{D}}\} = \frac{|\mathcal{S}\cap\bar{\mathcal{D}}|}{|\mathcal{S}|},$$

where $|\mathcal{S}| = 4R^2$ and $|\mathcal{S}\cap\bar{\mathcal{D}}|$ is deduced from Figures 6a and 6b. For $\ell = 1$, $|\mathcal{S}\cap\bar{\mathcal{D}}| = 2\bar{N}^{(e)}R^2\left(1-\frac{1}{2\beta}\right)^2$ with $\bar{N}^{(e)}$ being the average number of neighbors in (9). The case of $\ell = 2$ is more complexe as the number of neighbors that affect the area of $|\mathcal{S}\cap\bar{\mathcal{D}}|$ (not in a proportional way), as following:

$$|\mathcal{S}\cap\bar{\mathcal{D}}| = \begin{cases} A & \text{if } |\mathcal{N}(s_0)| = 4 \\ A - A_1 & \text{if } |\mathcal{N}(s_0)| = 3 \\ A - 2A_1 - A_2 & \text{if } |\mathcal{N}(s_0)| = 2. \end{cases}$$

with $A = R^2(4-\frac{1}{\beta^2})$, $A_1 = \frac{R^2}{\beta}(1-\frac{1}{2\beta})$ and $A_2 = R^2(1-\frac{1}{2\beta})^2$. It follows that,

$$\mathbb{E}[|\mathcal{S}\cap\bar{\mathcal{D}}|] = A - A_1\frac{2(2^{\frac{q-2}{2}}-1)}{2^{q-2}} - 2A_1\frac{1}{2^{q-2}} - A_2\frac{1}{2^{q-2}}. \quad (49)$$

The strict SER is then,

$$\mathbb{P}_e^{(e,2)} = (1-2^{-q})\left(1-\frac{1}{2\beta}\right)\left(1+\frac{1-2^{-q/2}}{1+2^{-q/2}}\frac{1}{2\beta}\right)$$

We should note that due to the cross-labeling applied to 64QAM, we have $\sqrt{\theta P}|(\psi(1101|11) - \psi(1101|00))| < 2R$ and also $\sqrt{\theta P}|(\psi(0111|10) - \psi(0111|01))| < 2R$, the SER expression will not detect that these two symbols correspond to the same binary information sequence. To take into account this event, we should include this particular case that arises with probability $1/2^{q-2}$, for which $|\mathcal{S}\cap\bar{\mathcal{D}}| = A - A_2$. By updating this expression,

$$\mathbb{E}[|\mathcal{S}\cap\bar{\mathcal{D}}|] = A - A_1\frac{2(2^{\frac{q-2}{2}}-1)}{2^{q-2}} - 2A_1\frac{1}{2^{q-2}} - A_2\frac{2}{2^{q-2}}.$$

A correction term should be then added to the SER as $\mathbb{P}_{e,c} = \mathbb{P}_e^{(e,2)} - 2^{-q}\left(1-\frac{1}{2\beta}\right)^2$.

B. Proof of Theorem 3

Assuming that the number of neighbors is equal to 4, the correct decision probability is,

$$\mathrm{P}_c = \left(\frac{1}{2R} \int_{-\frac{R}{\beta}}^{+\frac{R}{\beta}} \left[\Phi\Big(\frac{R - u_{z,1}}{\sigma_h} \Big) - \Phi\Big(-\frac{R + u_{z,1}}{\sigma_h} \Big) \right] du_{z,1} \right)^2 .$$

The expansion of this integral leads to,

$$\mathrm{P}_c = \left(\frac{1}{2^{\ell/2+1}\beta} (\mathrm{P}_{c,1} + P_{c,2}) \right)^2 ,$$

with

$$\mathrm{P}_{c,1} = -\eta_m \operatorname{erf}\left(\eta_m \sqrt{\frac{\mathrm{SNR}_h}{2}} \right) + \eta_p \operatorname{erf}\left(\eta_p \sqrt{\frac{\mathrm{SNR}_h}{2}} \right),$$

and

$$\mathrm{P}_{c,2} = \sqrt{\frac{2}{\pi\,\mathrm{SNR}_h}} \left[\exp\left(-\frac{\mu_p^2}{2}\,\mathrm{SNR}_h \right) - \exp\left(-\frac{\mu_m^2}{2}\,\mathrm{SNR}_h \right) \right].$$

This expression can be rewritten as,

$$\mathrm{P}_c = \Big(1 - \frac{1}{2^{\ell/2+1}\beta} \big(P_{e,1} + P_{e,2} \big) \Big)^2 \tag{50}$$

with $P_{e,1} = 2^{\ell/2+1}\beta - \mathrm{P}_{c,1}$ and $\mathrm{P}_{e,2} = -\mathrm{P}_{c,2}$. The expansion of these expressions leads to (31) and (32). Finally, the SER can be then rewritten as,

$$\mathrm{P}_e = 1 - \mathrm{P}_c \approx \frac{2}{2^{\ell/2+1}\beta} \big(P_{e,1} + P_{e,2} \big).$$

Due to the symmetry of the distribution function of u_z in Lemma 1, the average symbol error probability considering the number of neighbors $|\mathcal{N}_s|$ in Λ_k in (7) and (8) is $\mathbb{P}_e = \mathrm{P}_e \times \mathrm{Prob}\{|\mathcal{N}_s| = 4\} + \frac{3}{4}\mathrm{P}_e \times \mathrm{Prob}\{|\mathcal{N}_s| = 3\} + \frac{2}{4}\mathrm{P}_e \times \mathrm{Prob}\{|\mathcal{N}_s| = 2\} + \frac{1}{4}\mathrm{P}_e \times \mathrm{Prob}\{|\mathcal{N}_s| = 1\} = \frac{\mathbb{E}[|\mathcal{N}_s|]}{4}\mathrm{P}_e$.

C. Proof of Corollary 3.1

The expression in Corollary 3.1 is obtained by averaging the SER in Theorem 3 over all the values of the Rayleigh distributed variable $|h|$ with parameter $1/2$.

D. Proof of Corollary 3.2

Note that, for $\eta_m \neq 0$ and $\eta_p \neq 0$, $\bar{\mathbb{P}}_{s,1}(\mathrm{SNR})$ and $\bar{\mathbb{P}}_{s,2}(\mathrm{SNR})$ can be written as,

$$\bar{\mathbb{P}}_{s,1}(\mathrm{SNR}) = \eta_p \left[1 - \left(1 + \frac{1}{\eta_p^2\,\mathrm{SNR}_u} \right)^{-1/2} \right] - \eta_m \left[1 - \mathrm{sign}\big(\eta_m\big) \left(1 + \frac{1}{\eta_m^2\,\mathrm{SNR}_u} \right)^{-1/2} \right], \tag{51}$$

$$\bar{\mathbb{P}}_{s,2} = \frac{1}{\mathrm{SNR}} \left[\frac{1}{|\eta_m|} \left(1 + \frac{1}{\eta_m^2\,\mathrm{SNR}_u} \right)^{-1/2} - \frac{1}{\eta_p} \left(1 + \frac{1}{\eta_p^2\,\mathrm{SNR}_u} \right)^{-1/2} \right]. \tag{52}$$

Corollary 3.2 is deduced from the Taylor expansion of (51) and (52) in the neighborhood of ∞.

REFERENCES

[1] L. Mroueh and I. Ajayi, " Bit Interleaved and Coded Modulation with Indexed Partitions for Physical Layer Security, note= submitted to IEEE Military Communication 2024 ."

[2] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and Applications of Physical Layer Security Techniques for Confidentiality: A Comprehensive Survey," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 2, pp. 1773–1828, 2019.

[3] P. Angueira, I. Val, J. Montalbán, O. Seijo, E. Iradier, P. S. Fontaneda, L. Fanari, and A. Arriola, "A Survey of Physical Layer Techniques for Secure Wireless Communications in Industry," *IEEE Communications Surveys and Tutorials*, vol. 24, no. 2, pp. 810–838, 2022.

[4] F. Oggier, P. Solé, and J.-C. Belfiore, "Lattice Codes for the Wiretap Gaussian Channel: Construction and Analysis," *IEEE Transactions on Information Theory*, vol. 62, no. 10, pp. 5690–5708, 2016.

[5] R. A. Chou, "Explicit Wiretap Channel Codes via Source Coding, Universal Hashing, and Distribution Approximation, When the Channels' Statistics are Uncertain," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 117–132, 2023.

[6] H. Niu, M. Iwai, K. Sezaki, L. Sun, and Q. Du, "Exploiting fountain codes for secure wireless delivery," *IEEE Communications Letters*, vol. 18, no. 5, pp. 777–780, 2014.

[7] L. Sun and Q. Du, "A review of physical layer security techniques for internet of things: Challenges and solutions," *Entropy*, vol. 20, no. 10, p. 730, 2018.

[8] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless Information-Theoretic Security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

[9] T.-H. Nguyen, J. Louveaux, P. De Doncker, and F. Horlin, "Performance Analysis of Matched-Filter Precoded MISO-OFDM Systems in the Presence of Imperfect CSI," in *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, 2020, pp. 1–5.

[10] A. Mayouche, D. Spano, C. G. Tsinos, S. Chatzinotas, and B. Ottersten, "Learning-Assisted Eavesdropping and Symbol-Level Precoding Countermeasures for Downlink MU-MISO Systems," *IEEE Open Journal of the Communications Society*, vol. 1, pp. 535–549, 2020.

[11] S. Goel and R. Negi, "Guaranteeing Secrecy using Artificial Noise," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, 2008.

[12] B. Li, M. Zhang, Y. Rong, and Z. Han, "Artificial Noise-Aided Secure Relay Communication With Unknown Channel Knowledge of Eavesdropper," *IEEE Transactions on Wireless Communications*, vol. 20, no. 5, pp. 3168–3179, 2021.

[13] M. F. Marzban, R. Chabaan, N. Al-Dhahir, and A. El Shafie, "Securing OFDM-based wireless links using temporal artificial-noise injection," in *2018 15th IEEE Annual Consumer Communications and Networking Conference (CCNC)*, 2018, pp. 1–6.

[14] L. Y. Wang, T. and A. Vasilakos, "Survey on channel reciprocity based key establishment techniques for wireless systems," *Wireless Netw 21*, p. 1835–1846, 2015.

[15] P. Yadav, S. Kumar, and R. Kumar, "A comprehensive survey of physical layer security over fading channels: Classifications, applications, and challenges," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 9, p. e4270, 2021.

[16] F. Pan, Z. Pang, M. Luvisotto, M. Xiao, and H. Wen, "Physical-Layer Security for Industrial Wireless Control Systems: Basics and Future Directions," *IEEE Industrial Electronics Magazine*, vol. 12, no. 4, pp. 18–27, 2018.

[17] W.C. Jakes Jr., "Microwave Mobile Communications," in *Wiley-Interscience, New York*, 1974.

[18] G. Ungerboeck, "Channel coding with multilevel/phase signals," *IEEE Transactions on Information Theory*, vol. 28, no. 1, pp. 55–67, 1982.

[19] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "New Physical Layer Key Generation Dimensions: Subcarrier Indices/Positions-Based Key Generation," *IEEE Communications Letters*, vol. 25, no. 1, pp. 59–63, 2021.

[20] Y. E. H. Shehadeh and D. Hogrefe, "An optimal guard-intervals based mechanism for key generation from multipath wireless channels," in *2011 4th IFIP International Conference on New Technologies, Mobility and Security*. IEEE, 2011, pp. 1–5.

[21] Y. Wu, Y. Yu, Y. Hu, Y. Sun, T. Wang, and Q. Zhang, "Channel-Based Dynamic Key Generation for Physical Layer Security in OFDM-PON Systems," *IEEE Photonics Journal*, vol. 13, no. 2, pp. 1–9, 2021.