# Chip-Interleaved DSSS for Energy-Efficient Physical Layer Encryption

Clément Leroy, Tarak Arbi, Oudomsack Pierre Pasquero, Benoit Geller

# Chip-Interleaved DSSS for Energy-Efficient Physical Layer Encryption

Clément Leroy
*Department U2IS, ENSTA Paris*
*Institut Polytechnique de Paris, France*
clement.leroy@ensta-paris.fr

Tarak Arbi
*Department U2IS, ENSTA Paris*
*Institut Polytechnique de Paris, France*
tarak.arbi@ensta-paris.fr

Oudomsack Pierre Pasquero
*DGA-MI, French Ministry of Defense*
*35998 Rennes cedex 9, France*
oudomsack.pasquero@intradef.gouv.fr

Benoit Geller
*Department U2IS, ENSTA Paris*
*Institut Polytechnique de Paris, France*
benoit.geller@ensta-paris.fr

***Abstract*—Traditional methods for ensuring secure communications typically rely on encryption, which necessitates some form of coordination between the transmitter and the receiver. The Direct Sequence Spread Spectrum modulation can introduce some security at the physical layer but this technique must be combined with other technologies. Physical layer encryption techniques offer an alternative approach by taking advantage of transmit arrays to introduce beamformed noise. These techniques guarantee a certain level of confidentiality without requiring neither a heavy coordination nor losing time for secret key establishment, which make these techniques very attractive in particular for military and secured communications. However, the proposed solutions in the literature suffer from several limitations, and in particular, poor energy efficiency. To address this issue, we propose an original solution for physical layer encryption that does not spoil any energy with a signal mask by taking advantage of the wiretap channel inherent degradation introduced by the spatial chip interleaving over the transmitter antennas. Our simulations confirm that our proposal guarantees a considerable level of confidentiality without any energy loss.**

***Index Terms*—Physical layer encryption, Direct-Sequence Spread Spectrum (DSSS), Multiple Input Single Output (MISO)**

## I. Introduction

To ensure the confidentiality of communications, cryptography techniques, such as the Advanced Encryption Standard (AES) [1], are traditionally employed as they offer high confidentiality level. However, these techniques require prior key sharing in order to cipher and decipher the transmitted information. Agreeing upon this key requires coordination and infrastructure, which, in certain scenarios, may not align with the requirements of tactical communication. Additionally, perfect secrecy can only be guaranteed if the key size matches the size of the transmitted information [2].

The Direct Sequence Spread Spectrum (DSSS) technique is traditionally known to bring some form of security at the physical level [3]. However, even with the use of non-linear sequences to counter the technology progresses available for eavesdroppers, the security of DSSS is enhanced when used jointly with other techniques [4], [5], such as rotated constellations [6]–[11]. Physical Layer Encryption (PLE) is a cutting-edge approach which aims at circumventing the key sharing problem in wireless communications by taking advantage of the physical transmission medium [12]. Wyner laid the foundations of these techniques [13] by proving that it was possible to transmit information with perfect secrecy as long as the legitimate transmission channel has a larger capacity than the illegitimate channel. Unlike traditional encryption methods that focus on securing the content of data, physical layer encryption focuses on protecting the transmitted signal. Physical layer security techniques can provide an additional layer of security against eavesdropping and can be combined with classical cryptography. This approach shows great potential for ensuring secure and robust communication.

In particular, spatial encryption is a method that leverages the physical space encompassing transmission. By utilizing the inherent properties of the surrounding environment, such as spatial proximity and locality, spatial encryption offers an additional level of security against unauthorized access and data breaches. Consequently, it transforms communication security into a physical security concern, necessitating the adaptation of the transmitted signal by the transmitter. This adaptation ensures that only receivers in the legitimate receiver direction can receive non-degraded observations of the transmitted information symbols.

The authors in [14] proposed a method to degrade the illegitimate channel without prior knowledge of the eavesdropper's location. This approach involves introducing random Gaussian noise into the kernel of the legitimate transmission channel. Consequently, the intended receiver accurately receives the information, while an eavesdropper receives a degraded version of transmitted signal due to the artificial noise introduced by the transmitter. This lead to a significant reduction of the wiretap channel capacity, without impacting the capacity of

This study was funded by the AID CIEDS project SEPHYTEL.

the primary channel. [15] further refined this method by investigating the optimal energy level to introduce in the masking process, with the aim of maximizing the secrecy-capacity. However, the addition of an artificial Gaussian noise leads to a significant variation in the energy required for transmission with a high Peak-to-Average Power Ratio (PAPR). Alternative masking techniques, such as directional modulation (DM), have been devised [16] [17] to intentionally distort the received constellation for the eavesdropper. However, these techniques suffer from similar limitations. Alternatively, [18] addresses the particular case of a multi-antenna system and proposes a novel method to generate the mask signal that leads to a low PAPR. This method requires reserving some of the transmission power to send a mask signal and its theoretical performance has not been studied by the authors in [18].

In this paper, we propose a novel PLE technique: Chip-Interleaved Direct Sequence Spread Spectrum (DSSS). According to our simulations, interleaving the chips of the DSSS signals over the transmission antennas, our method considerably degrades the wiretap channel leading to a secrecy rate close to the channel capacity. In contrast to [14], [18], the energy efficiency of the proposed method is optimal as it does not require any additional energy, as for instance with mask signal methods.

The reminder of this paper is organized as follows. Section II details the proposed encryption method. Section III analyze the performance of the method proposed in terms of Signal to Interference and Noise ratio (SINR) and secrecy capacity. Some numerical results are presented in Section IV, and finally Section V concludes the paper.

## II. Our proposed encryption technique

We now describe the system model depicted in Fig.1. In this paper, we assume a MISO (Multiple Input, Single Output) communication system with $L$ transmit antennas. We assume that those $L$ antennas are aligned and symmetrically spaced along the y-axis at a distance $d$. First, the information bits are eventually coded [19] and then transformed into a sequence of symbols $(a_1, a_2, ...)$ belonging to a given constellation such as the QAM constellation. Thereafter, the information symbols are divided into blocks of $L$ symbols $(a_1(p), a_2(p), ..., a_L(p))$, where $p$ is the block index. To simplify the notation, the block index is dropped in the sequel of this paper. The transmitter spreads each information symbol $a_l$ of the block by a spreading sequence $\mathbf{b}_l = (b_1^{(l)}, b_2^{(l)}, ..., b_N^{(l)})$ where $N$ denotes the spreading factor. It is important to note that the confidentiality of our method does not rely on the spreading sequence, which we assume to be known by the illegitimate receiver. Obviously, additional security is gained in the scenario where the eavesdropper lacks knowledge of the sequences employed, in particular, with time-varying spreading sequences.

At chip time instant $n$, the chips to be transmitted are $(a_1 b_n^{(1)}, a_2 b_n^{(2)}, ..., a_L b_n^{(L)})$. Instead of sending $a_l b_n^{(l)}$ on the $l$-th antenna, we propose a spatial interleaving by transmitting on the $l$-th antenna the chip $a_{\sigma_n(l)} b_n^{(\sigma_n(l))}$, where $\sigma_n$ is a random permutation. It is worth noting that these permutations vary at each time instant $n$, and the transmitter is the only one to know how the chips are interleaved as the legitimate receiver does not need to know it to properly decode the transmitted information symbols. The transmitted signal on antenna $l$ at chip time instant $n$ can thus be expressed as:

$$s_l(n) = w_l a_{\sigma_n(l)} b_n^{(\sigma_n(l))}, \tag{1}$$

where $w_l$ is the beamforming weight of the $l$-th antenna. Without loss of generality, assuming that the legitimate receiver is positioned at $\theta = 0$, we set $w_l = 1$ for all $l$ to align the boresight of the array with the $x$-axis. However, by adjusting the beamforming weights, the proposed method can be used for any scenario where the legitimate receiver is located in another direction than than $\theta = 0$.

Considering an Additive White Gaussian Noise (AWGN) channel and assuming perfect synchronization [19]–[22], the received signal at chip time instant $n$ and at angle $\theta$ off the $x$-axis is:

$$r_n(\theta) = \gamma \sum_{l=1}^{L} a_{\sigma_n(l)} b_n^{(\sigma_n(l))} e^{j\phi(l-1)} + \nu_n, \tag{2}$$

where $\phi = 2\pi \frac{d}{\lambda} sin(\theta)$, $\lambda$ is the wavelength, $\nu_n$ is a Gaussian noise and $\gamma$ is the attenuation factor omitted in the following for the sake of clarity. For the intended receiver, it is clear that the interleaving introduced by the transmitter has no impact on the reception quality as for $\theta = 0$, the received symbol at chip time instant $n$ can be written as:

$$\begin{aligned} r_n(\theta = 0) &= \sum_{l=1}^{L} a_{\sigma_n(l)} b_n^{(\sigma_n(l))} + \nu_n \\ &= \sum_{l=1}^{L} a_l b_n^{(l)} + \nu_n. \end{aligned} \tag{3}$$

Thus, after receiving all the chips, the legitimate receiver can decode the symbol $a_k$ by multiplying the received symbols and the corresponding spreading sequence $\mathbf{b}^{(k)}$:

$$\begin{aligned} \mathbf{r}(\theta = 0)^T \mathbf{b}^{(k)} &= \begin{bmatrix} r_1(0) & r_2(0) & \dots & r_N(0) \end{bmatrix} \cdot \begin{bmatrix} b_1^{(k)} \\ b_2^{(k)} \\ \vdots \\ b_N^{(k)} \end{bmatrix} \\ &= a_k + \nu_k, \end{aligned} \tag{4}$$

where is equal to $\sum_{n=1}^{N} b_n^{(k)} \nu_n$.

For the illegitimate receiver however, the decoding is not as trivial. He indeed receives:

$$r_n(\theta \neq 0) = \sum_{l=1}^{L} (a_{\sigma_n(l)} b_n^{(\sigma(l))} e^{j\phi(l-1)} + \nu_n). \tag{5}$$

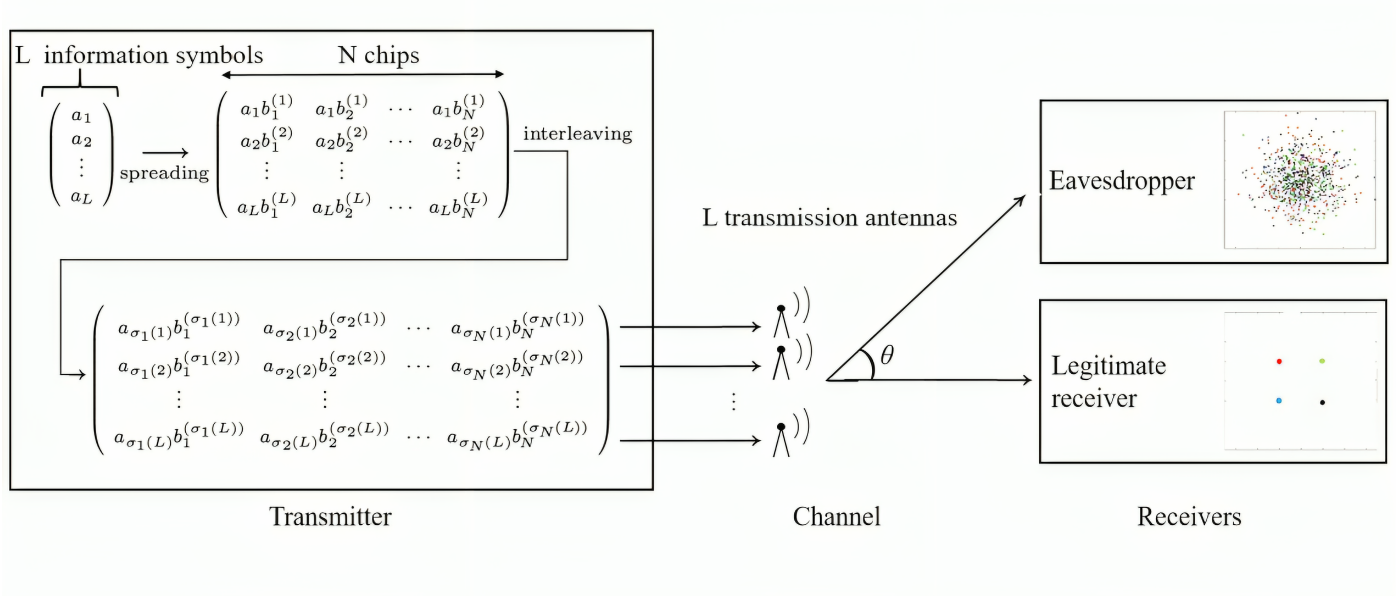



Fig. 1: Summary of the method.

The interleaving has considerable impact and leads to inter-symbol interference as the exponential term breaks the orthogonality between the spreading sequences. Indeed, after despreading, the illegitimate receiver obtains:

$$\begin{aligned}\mathbf{r}(\theta \neq 0)^T \mathbf{b}^{(k)} &= \sum_{n=1}^{N} \left( \sum_{l=1}^{L} a_{\sigma_n(l)} b_n^{(\sigma(l))} e^{j\phi(l-1)} + \nu_n \right) b_n^{(k)} \\ &= \sum_{l=1}^{L} a_l \sum_{n=1}^{N} b_n^{(l)} b_n^{(k)} e^{j\phi(\sigma_n^{-1}(l)-1)} + \sum_{n=1}^{N} \nu_n b_n^{(k)}.\end{aligned} \tag{6}$$

Note that the exponential term added to the sum by our method leads inevitably to Inter-Symbol Interference (ISI) as illustrated by section V.

## III. Performance analysis

In this section, we develop a theoretical framework to assess the performance of our proposal.

### A. Signal to Interference and Noise Ratio (SINR)

In this paper, we assume that the spreading sequences are orthogonal. However, due to the proposed spatial interleaving introduced at the transmitter, these spreading sequences remains orthogonal only for $\theta = 0$. Indeed, for $\theta \neq 0$, the despreaded signal (see eq. 4) can be developed as:

$$\begin{aligned}\mathbf{r}(\theta \neq 0) * \mathbf{b}^{(k)} = &\underbrace{a_k \frac{1}{N} \sum_{n=1}^{N} e^{j\phi(\sigma_n^{-1}(k)-1)}}_{\textit{Information}} + \underbrace{\sum_{n=1}^{N} \nu_n b_n^{(k)}}_{\textit{Noise}} \\ &+ \underbrace{\sum_{1 \leq l \leq L, l \neq k} a_l \sum_{n=1}^{N} b_n^{(l)} b_n^{(k)} e^{j\phi(\sigma_n^{-1}(l)-1)}}_{\textit{Intersymbol Interference}}.\end{aligned} \tag{7}$$

In equation (5), the spreading sequences are normalized with unit energy such that $(b_n^{(l)})^2 = \frac{1}{N}$ for all $n$ and $l$. It can be observed that the received signals is the superposition of three components: the information symbol, the Intersymbol Interference (ISI), and a noise term. Consequently, the SINR can be expressed as:

$$\begin{aligned}&\mathrm{SINR}(\theta) = \\ &\frac{1}{L} \sum_{k=1}^{L} \mathbb{E}_{\mathbf{a}} \frac{\left| a_k \frac{1}{N} \sum_{n=1}^{N} e^{j\phi(\sigma_n^{-1}(k)-1)} \right|^2}{\left| \sum_{\substack{1 \leq l \leq L \\ l \neq k}} a_l \sum_{n=1}^{N} b_n^{(l)} b_n^{(k)} e^{j\phi(\sigma_n^{-1}(l)-1)} \right|^2 + 2N_0},\end{aligned} \tag{8}$$

where $\mathbb{E}$ denotes the expectation, $N_0$ is the unilateral power spectrum density of the noise and $\sigma_i$ is an index permutation. The SINR can be upper bounded as:

$$\mathrm{SINR}(\theta) \leq \frac{\mathbb{E}_k(|a_k|^2)}{2N_0} = \mathrm{SNR}. \tag{9}$$

In section V, we show that the SINR for $\theta \neq 0$ is considerably lower than the SNR for $\theta = 0$ (i.e. no ISI).

### B. Secrecy capacity over the AWGN channel

The secrecy capacity $C_s(\theta)$ quantifies the maximum amount of information that can be securely and reliably transmitted from the sender to the intended receiver, considering the presence of a passive eavesdropper located in the direction $\theta$. It can be lower bounded as follows [23], [24]:

$$C_s(\theta) \geq \overline{C_s}(\theta) = I(\mathbf{a}, \mathbf{r}(0)) - I(\mathbf{a}, \mathbf{r}(\theta)), \tag{10}$$

where $I(\mathbf{A}, \mathbf{r}(\theta))$ denotes the mutual information between the information symbols and the received symbols. It can be developed as:

$$\begin{aligned} & I(\mathbf{a}, \mathbf{r}(\theta)) \\ & = \sum_{\mathbf{a} \in \mathcal{X}^L} \int_{\mathbf{r} \in \mathbb{C}^N} P(\mathbf{a}, \mathbf{r}) log_2 \left( \frac{P(\mathbf{a}, \mathbf{r})}{P(\mathbf{a})P(\mathbf{r})} \right) d\mathbf{r} \\ & = \sum_{\mathbf{a} \in \mathcal{X}^L} \int_{r \in \mathbb{C}^N} P(\mathbf{a})P(\mathbf{r}|\mathbf{a}) log_2 \left( \frac{P(\mathbf{r}|\mathbf{a})}{P(\mathbf{r})} \right) d\mathbf{r} \\ & = \mathbb{E}_{\mathbf{a},\mathbf{r}}[log_2(f(\mathbf{a}, \mathbf{r})], \end{aligned} \tag{11}$$

where $\mathcal{X}$ is the constellation symbol, and :

$$f(\mathbf{a}, \mathbf{r}) = \frac{\sum_{\boldsymbol{\sigma}} P(\boldsymbol{\sigma})P(\mathbf{r}|\mathbf{a}, \boldsymbol{\sigma})}{\mathbb{E}_{\tilde{\mathbf{a}}}[\sum_{\boldsymbol{\sigma}} P(\boldsymbol{\sigma})P(\mathbf{r}|\tilde{\mathbf{a}}, \boldsymbol{\sigma})]}, \tag{12}$$

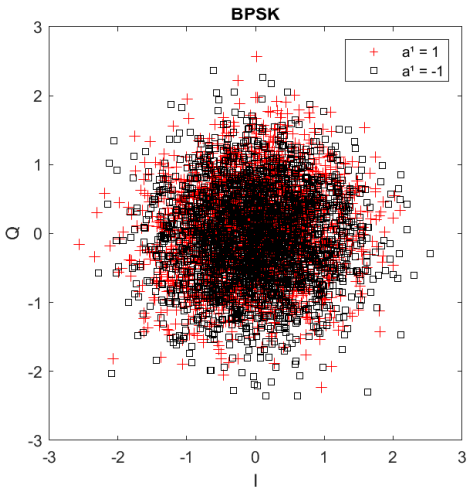
where $\boldsymbol{\sigma}$ is a set of N permutations of N indexes. For an AWGN channel:

$$P(\mathbf{r}|\mathbf{a}, \boldsymbol{\sigma}) \propto exp \left( \frac{\sum_{n=1}^{N} |r_n(\theta) - \sum_{l=1}^{L} a_l b_n^{(l)} e^{j\phi(\sigma_n^{-1}(l)-1)}|^2}{4N_0} \right) \tag{13}$$

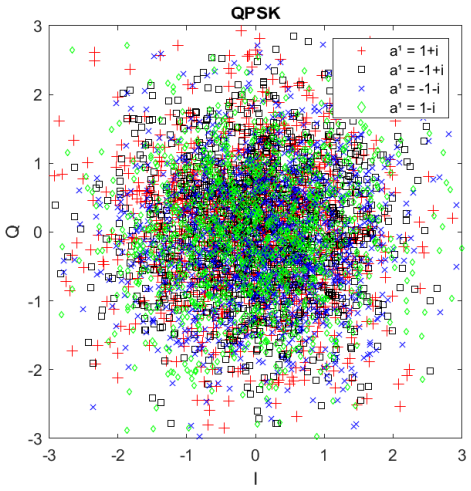
The quantities (11) and (12) can be evaluated through Monte-Carlo simulation (see section V, Figure 5).

It's worth noting that in scenarios where the eavesdropper enjoys theoretical advantages such as a noiseless wiretap channel, awareness of their position relative to the transmitter, and knowledge of the spreading sequences; confidentiality cannot be guaranteed in theory. However, this does not reflect the practical challenges an eavesdropper faces to recover the information symbols transmitted. As an example, Figure 2.a and 2.b show the I/Q diagram after despreading with spreading sequence $b^{(1)}$ for an illegitimate receiver at direction $\theta = 45°$, for spreading factor $N = 16$ and $L = 16$ antennas, over a noiseless channel and for BPSK and QPSK modulations respectively. The Monte-Carlo to obtain this figure is fixed to $10^3$.

In constrast to the legitimate receiver for which the I/Q diagram contains two symbols for BPSK and four symbols for QPSK, the I/Q diagram for an illegitimate receiver contains $Card(\mathcal{X})^L(L!)^N$ different symbols; for instance, with $L = N = 16$ and the BPSK modulation, the I/Q diagram contains $10^{218}$ symbols. Therefore, even with a noiseless channel, decoding the despreaded information symbol requires a prohibitive computing capacity.




(a) BPSK.




(b) QPSK.

Fig. 2: Received symbols after despreading obtained over a noiseless channel ($N_0 \to 0$).

## IV. Simulation results

In all simulations, we keep the ratio $\frac{d}{\lambda}$ fixed at $\frac{1}{4}$, and we use Hadamard orthogonal sequences as spreading sequences.

### A. Signal to Interference and Noise Ratio

Figure 3 (resp. Figure 4) illustrates, for the QPSK modulation with $L = 16$ antennas (resp. $L = 32$ antennas), the SINR as a function of the reception angle for several spreading factors $N$, and SNR (i.e. for $\theta = 0$) fixed at 5 dB.

The maximum value of the SINR is consistently achieved at 0 degree, as indicated by equation (7). Notably, this maximum does not depend on the value of $N$. As one deviates from the angle associated with the legitimate receiver's position, the SINR gradually decreases. Furthermore, we can observe that for the illegitimate receiver, the SINR is at least about 15 dB lower than the intended receiver SINR. The $L = 16$

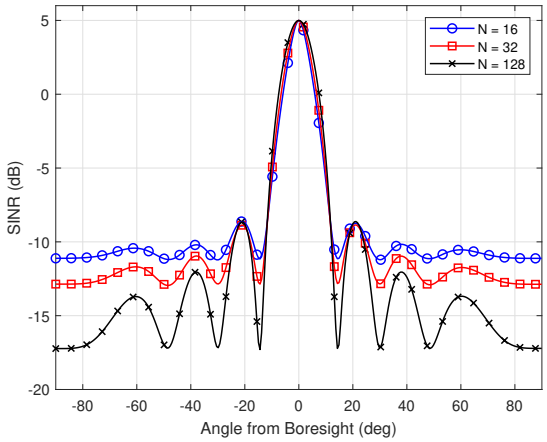



Fig. 3: SINR comparison for several spreading factors $N$ with the QPSK modulation and $L = 16$ antennas.

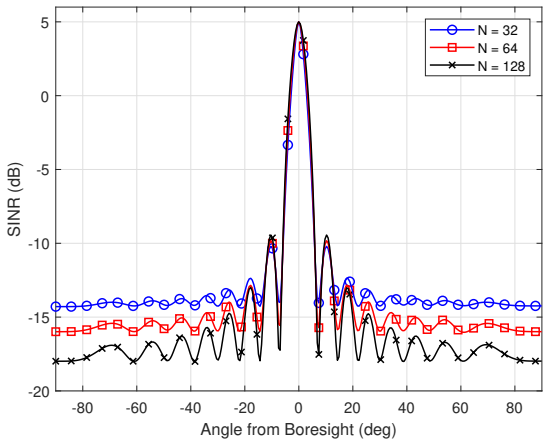



Fig. 4: SINR comparison for several spreading factors $N$ with the QPSK modulation and $L = 32$ antennas.

configuration exhibits an approximate width of the 6 dB main lobe of 17°, whereas for $L = 32$, it is merely 7°.

### B. Secrecy Capacity

Figure 5 depicts the minimum secrecy capacity obtained over an AWGN channel and with the BPSK constellation, where both the illegitimate and intended receivers experience the same Gaussian noise variance. The SNR is fixed to 3 dB. This secrecy capacity is compared to the mutual information between the transmitted symbols and the received signal by the legitimate receiver [2]. The secrecy capacity is nearly zero when the eavesdropper is positioned at the same angle as the legitimate receiver, as the eavesdropper then receives the same signal as the intended receiver. The secrecy capacity substantially increases as the angle widens. It approaches the maximum capacity of the channel as the angle expands. Similar results were obtained with other simulations parameters $(N, L, \mathcal{X})$.

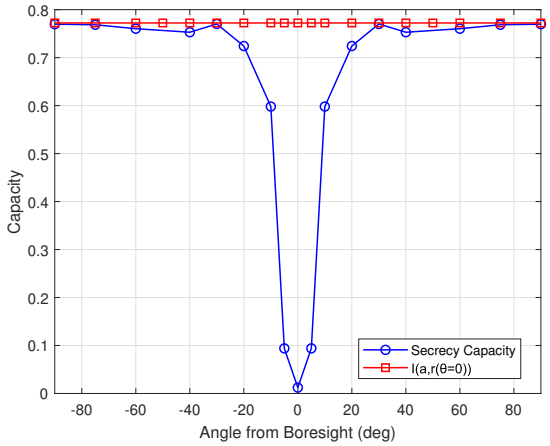



Fig. 5: Secrecy Capacity (SC) vs receiving angle at SNR $= 3$ dB

### C. Bit-Error Rate (BER) performance

Figure 6 shows the BER performance versus the angle for our method and several techniques proposed in the literature: artificial noise [14] and Out-Phased Array Linearized Signaling (OPALS) technique presented in [18], which addresses secure communication in a similar transmission system. The BER of our method does not present any lobe potentially vulnerability to an eavesdropper and does not need any additional energy requirement as we choose $N = L$, unlike OPALS and the artificial noise method. Moreover, the receiving angle is narrower, making the communication more secured.

Figure 7 shows the BER performance obtained with several constellation sizes, with $L = N = 16$. Our proposed method is slightly more efficient as the constellation size increases.

Finally, Figure 8 compares our method to the OPALS method [18] for the QPSK constellation QPSK and $L = N = 16$. OPALS is based on the addition of a mask signal to the transmitted signal; the energy cost of this mask signal increases as $R^2_{\max}$ increases. We can observe that our method achieves comparable results to OPALS for $R^2_{\max} = 6$; which represents a considerable energy loss for this method.

## V. Conclusion

This paper proposes a novel physical layer encryption technique. It is based on the joint use of DSSS and chip-interleaving over the transmitter antennas. To ensure a fair comparison with the state-of-the-art solution, the spreading sequences in this study are assumed to be known by the eavesdropper. Simulations of the SINR, the BER, and the secrecy capacity illustrate that the proposed method effectively degrades the wiretap channel without the need for adding artificial noise to mask the information signal, thereby eliminating energy loss. Therefore, our proposal could be a physical encryption candidate for future military communication systems, and even more, various wireless systems could benefit from the

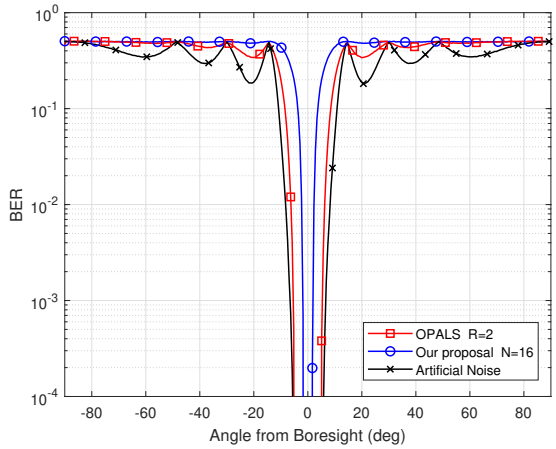



Fig. 6: BER comparison between the proposed method (QPSK, N=L=16), OPALS [18] and Artificial Noise Masking [14]

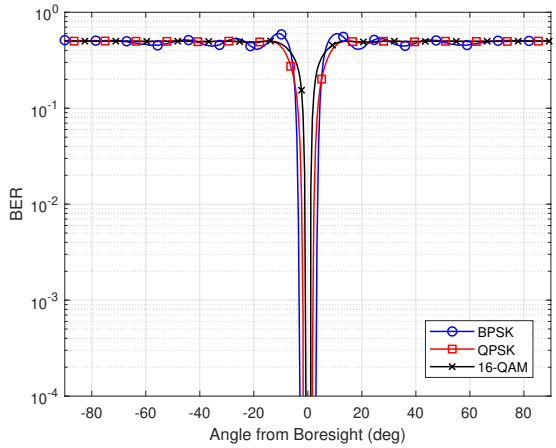



Fig. 7: BER obtained with various constellations

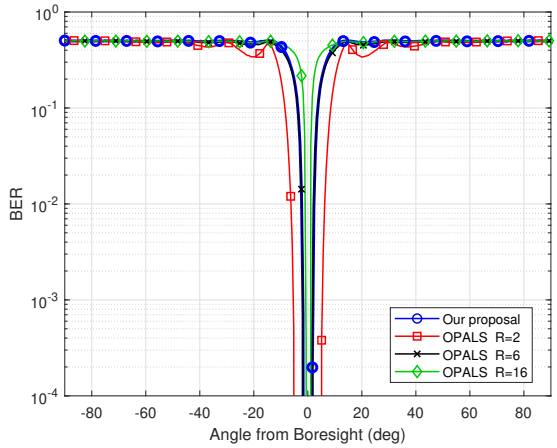



Fig. 8: BER comparison between the proposed method (QPSK, N=L=16) and various parameters of OPALS

significant level of confidentiality achieved without incurring any energy loss.

## REFERENCES


[1] J. Daemen, V. Rijmen, "The Design of Rijndael: The Advanced Encryption Standard" 2nd ed. Springer, 2020.

[2] C.E.Shannon, "Communication theory of secrecy systems", Bell Syst. Tech. J., vol. 28, pp. 656-715, 1949.

[3] D. Torrieri, "Principles of Spread Spectrum communication systems", 5th ed., Springer, 2022.

[4] D. Roque and C. Poulliat, "SNR-Optimal Spreading Sequences for Chip-Wise Faster-Than-Nyquist Signaling," in IEEE Communications Letters, vol. 27, no. 6, pp. 1594-1598, June 2023.

[5] Fei Wei, Shilian Zheng, Xiaoyu Zhou, Luxin Zhang, Caiyi Lou, Zhijin Zhao, Xiaoniu Yang, "Detection of Direct Sequence Spread Spectrum Signals Based on Deep Learning", *IEEE Transactions on Cognitive Communications and Networking*, 8 (3), 2022.

[6] T. Arbi, B. Geller, O. P. Pasquero "Direct-Sequence Spread Spectrum with Signal Space Diversity for High Resistance to Jamming", IEEE Milcom, San Diego, Nov. 2021.

[7] T. Arbi, B. Geller, J. Yang, C. Abdel Nour, O. Rioul, "Uniformly projected RCQD QAM: A low-complexity signal space diversity solution over fading channels with or without erasures", *IEEE Transactions on Broadcasting*, pp. 803-815, 64 (4), April 2018.

[8] Z. Ye, T. Arbi, F. -X. Socheleau and B. Geller, "Fast Soft Demapping for Underwater Acoustic Communications With Signal Space Diversity," *OCEANS 2018 MTS/IEEE* Charleston, SC, USA, 2018, pp. 1-6.

[9] J. Yang, M. Li, M. Li, C. Abdel Nour, C. Douillard, B. Geller, "Max-log demapper architecture design for DVB-T2 rotated QAM constellations", *IEEE Workshop on Signal Proc. Systems SiPS 2015* , pp. 1-6, Oct. 2015.

[10] T. Arbi, Z. Ye and B. Geller, "Low-Complexity Blind PAPR Reduction for OFDM Systems With Rotated Constellations," *IEEE Transactions on Broadcasting*, 67 (2), pp. 491-499, June 2021.

[11] J. Yang, K. Wan, B. Geller, C. Abdel Nour, O. Rioul, C. Douillard, "A low-complexity 2D signal space diversity solution for future broadcasting systems", IEEE *International Conference on Communications ICC 2015*, pp. 2762-2767, June 2015.

[12] A.Mukherjee, S.Fakoorian, J.Huang, and A.Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey." IEEE Communications Surveys Tutorials, 16 (3), pp. 1550-1573, Third 2014.

[13] A.Wyner, "The wire-tap channel", *The Bell System Technical Journal*, Volume: 54, Issue: 8, October 1975.

[14] Satashu Goel, and Rohit Negi, "Guaranteeing Secrecy using Artificial Noise", *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180-2189, June 2008.

[15] Gan Zheng, Pantelis-Daniel Arapoglou, and Björn Ottersten, "Physical Layer Security in Multibeam Satellite Systems", *IEEE Transactions on Wireless Communications*, vol. 11, no. 2, pp. 852-863, February 2012.

[16] M. Dally and J. Bernhard, "Directional modulation and coding in arrays," *IEEE Int. Sym. on Antennas and Propagation*, pp. 1984-1987, July 2011.

[17] V. Pellegrini, F. Principe, G. de Mauro, R. Guidi, V. Martorelli, and R. Cioni, "Cryptographically secure radios based on directional modulation" in International Conference on Acoustics,Speech and Signal Processing ICASSP 2014, May 2014.

[18] E. Tollefson, B.R. Jordan Jr, and J.D. Gaeddert, "Out-phased Array Linearized Signaling (OPALS): A practical Approach to Physical Layer Encryption" *MILCOM 2015, IEEE Military Communications Conference,*, 26-28 October 2015.

[19] B. Geller, I. Diatta, J.P. Barbot, C. Vanstraceele, F. Rambeau, "Block turbo codes: From architecture to application", *IEEE International Symposium on Information Theory ISIT 2006*, pp. 1813–1816, Aug. 2006.

[20] I. Nasr, L. Najjar Atallah, S. Cherif, B. Geller, "Near map dynamical delay estimator and bayesian CRB for coded QAM signals", *IEEE Trans. on Wireless Communications*, pp. 636-651, 17 (1), Jan. 2018.

[21] I. Nasr, L. Najjar Atallah, S. Cherif, B. Geller, J. Yang, "A soft maximum likelihood technique for time delay recovery", *International Conference on Communications and Networking*, 1-5, Mar. 2014.

[22] J. Yang, B. Geller and T. Arbi, "Proposal of a multi-standard transceiver for the WBAN Internet of Things," *Inter. Symposium on Signal, Image, Video and Communications*, Tunis, Tunisia, pp. 369-373, Sept. 2016.

[23] I. Csiszar and J. Korner, "Broadcast channels with confidential messages", IEEE Trans. Inform. Theory, vol. 24 (3), pp 339-348, May 1978.

[24] E. Telatar, "Capacity of multi-antenna Gaussian channels", Eur. Trans. Telecom. ETT, vol. 10, no 6, pp 585-596, Nov. 1999.