Multi-Domain Polarization for Enhancing the Physical Layer Security of MIMO Systems

Luping Xiang, *Member, IEEE*, Yao Zeng, *Student Member, IEEE*, Jie Hu, *Senior Member, IEEE*, Kun Yang, *Fellow, IEEE* and Lajos Hanzo, *Life Fellow, IEEE*

***Abstract*—A novel Physical Layer Security (PLS) framework is conceived for enhancing the security of the wireless communication systems by exploiting multi-domain polarization in Multiple-Input Multiple-Output (MIMO) systems. We design a sophisticated key generation scheme based on multi-domain polarization, and the corresponding receivers. An in-depth analysis of the system's secrecy rate is provided, demonstrating the confidentiality of our approach in the presence of eavesdroppers having strong computational capabilities. More explicitly, our simulation results and theoretical analysis corroborate the advantages of the proposed scheme in terms of its bit error rate (BER), block error rate (BLER), and maximum achievable secrecy rate. Our findings indicate that the innovative PLS framework effectively enhances the security and reliability of wireless communication systems. For instance, in a 4×4 MIMO setup, the proposed PLS strategy exhibits an improvement of 2dB compared to conventional MIMO, systems at a BLER of $2 \cdot 10^{-5}$ while the eavesdropper's BLER reaches 1.**

***Index Terms*—Physical layer security (PLS), multi-domain polarization, MIMO, secrecy code construction**

I. Introduction

To enhance the security of wireless communication systems, traditional approaches have primarily relied on secret key based encryption techniques at the network layer. However, the high computational burden of these methods has prompted researchers to explore secure transmission methods at the physical layer (PHY) [1, 2]. Physical layer security (PLS) based mechanisms can be broadly categorized into two groups: keyless PLS transmission techniques based on Wyner's theory [3] and key-based PLS transmission techniques rooted in Maurer's theory [4]. By appropriately integrating these techniques with modulation schemes and channel coding, the security of the system can be improved, while maintaining communication efficiency.

Keyless PLS techniques by definition operate without the need for a key, utilizing sophisticated signal processing methods to degrade the eavesdropper's (E) channel state, while simultaneously enhancing the quality of the legitimate communication channel. The concept of constructive interference, introduced in [5], relies on the transmission of directional artificial noise (AN) to interfere with E. In [6], symbol-level transmit pre-encoders (TPC) are employed for reducing the transmitter's energy consumption and for enhancing the system's overall performance while jamming E. Considering angular errors, Hu *et al.* [7] derive a closed-form expression for the AN projection matrix, assuming realistic directional angular estimation errors obeying a uniform distribution within a practical range. Xu *et al.* [8] designs an effective Artificial Noise Assisted Security Scheme (ANAS), relying on two phases of transmission: in Phase 1, the legitimate parties send two independent artificial noise sequences (ANs), while in Phase 2, the transmitter superimposes the ANs received in Phase 1 on the signals and transmits the resultant sequences mixed signal. Secure communication is achieved since the ANs superimposed on the legitimator, signal in phase 2 can be effectively cancelled by the legitimate receiver while still interfering with the eavesdropper. Shu *et al.* [9] present a robust, AN-based multi-beam broadcast system capable of improving both the security and the rate. Although AN-based keyless designs succeed in increasing the secure transmission rates, this is achieved at the cost of increased complexity and peak to average power ratio (PAPR).

The family of key-based PLS transmission techniques has also garnered interest from numerous researchers [10, 11]. Key generation methods exploit the random physical layer attributes of the channel [12] to prevent E from gleaning confidential information from the legitimate links [13–15]. The legitimate user employs traditional channel estimation techniques for acquiring the channel state information (CSI) of the legitimate link and subsequently generates the physical layer key [16, 17]. By contrast, E is unable to access the CSI of the legitimate link and the associated key. However, CSI-based key generation schemes are challenging to implement in practice due to biases introduced by channel estimation. This issue has been mitigated through the development of high-performance secure channel coding techniques [18].

In conventional communication systems, coding and encryption are treated as separate processes, where physical layer coding is harnessed for enhancing the reliability [25], while upper layer encryption is used for ensuring security [26]. For circumventing the weaknesses of upper layer encryption,

This work was supported in part by MOST Major Research and Development Project under Grant 2021YFB2900204; in part by the Sichuan Major R&D Project under Grant 22QYCX0168; in part by the Sichuan Science and Technology Program under Grant 2022YFH0022 and Grant 2023NSFSC1375; in part by the Natural Science Foundation of China under Grant 62132004, Grant 61971102 and Grant 62301122; in part by the Stable Supporting Fund of National Key Laboratory of Underwater Acoustic Technology; and in part by the Key Research and Development Program of Zhejiang Province under Grant 2022C01093. (*Corresponding Author: Jie Hu.*)

L. Hanzo would like to acknowledge the financial support of the Engineering and Physical Sciences Research Council projects EP/W016605/1, EP/X01228X/1 and EP/Y026721/1 as well as of the European Research Council's Advanced Fellow Grant QuantCom (Grant No. 789028)

Luping Xiang, Yao Zeng and Jie Hu are with the School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China, email: luping.xiang@uestc.edu.cn, 202122010522@std.uestc.edu.cn, hujie@uestc.edu.cn.

Kun Yang is with the School of Computer Science and Electronic Engineering, University of Essex, Essex CO4 3SQ, U.K., e-mail: kunyang@essex.ac.uk.

Lajos Hanzo is with the School of Electronics and Computer Science, University of Southampton, Southampton SO171BJ, U.K., e-mail: lh@ecs.soton.ac.uk

TABLE I: Boldly contrasting our novelty to the literature

Contributions	ours	[1, 2]	[3]	[4, 19–21]	[5, 6]	[7, 9]	[12]	[16, 17]	[22]	[23]	[24]
Multiple mapping patterns	✔							✓			
Physical layer security (PLS)	✔	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Reduce receiver latency	✔					✓					✓
Secrecy rate analysis	✔			✓		✓	✓	✓	✓	✓	✓
MIMO polarization	✔										
Detection of sequential mapping coding construction	✔										

researchers have embarked on investigating the joint design of coding and encryption at the physical layer [27]. This approach is eminently suitable for wireless channels upon using appropriate coding schemes, for simultaneously improving the legitimate link and for preventing E from accessing any confidential information. Powerful low-density parity-check (LDPC) codes are particularly suitable for secure channel coding design. In this context, Li *et al.* [22] proposes an LDPC-based McEliece secrecy coding scheme for enhancing the information reliability of legitimate users and the information security against E. Motamedi *et al.* [28] examine the-perfect-security' physical layer authentication problem of wireless networks using LDPC codes and hash functions, achieving high authentication rates in the presence of an E having high computational power.

Additionally, the integration of polar codes [29] and physical layer security has garnered widespread scholarly attention [30, 31]. Polar codes, conceived by Arikan [32], achieve symmetric capacity for binary input memoryless channels (BMCs). In [23], a concatenated coding scheme combining polar codes and fountain codes is proposed by Yang and Zhuang for memoryless erasure binary eavesdropping channel models, while relying on finite code lengths for ensuring security. Hao *et al.* [33] discuss a secure transmission scheme employing two-dimensional polar codes designed for block fading eavesdropping channels, in the face of instantaneous secrecy capacity fluctuations. Bao *et al.* [24] combine polar codes with artificial noise to derive upper and lower bounds of the symmetric capacity for polarized bit channels, which benefit the legitimate receiver but not the eavesdropper.

The core of polar code construction lies in the so-called channel polarization processing detailed in [34]. As the coding space dimension approaches infinity, all sub-channels become fully polarized. However, under practical finite code lengths, many sub-channels remain partially polarized, hence impacting the system's secrecy rate. To address this issue, we explore the introduction of multi-domain polarization into physical layer security research. Dai *et al.* [35], guided by the concept of generalized polarization, propose a polarization-coded MIMO model that significantly enhances the benefits of polarization. Explicitly, they demonstrate that multi-domain polarization is eminently suitable for PLS-enhancement.

In this context, we jointly design multi-domain polarization and encryption. On one hand, MIMO detection schemes apply different processing methods and detection orders for the individual spatial layers, resulting in varying signal reliability. Based on this, we design a random detection order based multi-domain polarization model that prevents eavesdroppers from inferring with the legitimate link's MIMO detection mode or multi-domain polarization process, leading to extremely high eavesdropper decoding error rates. On the other hand, since the time-division duplex (TDD) systems' channel reciprocity prevents eavesdroppers from obtaining the legitimate link's instantaneous gain, we partition the gain range into multiple contiguous but non-overlapping intervals. Based on this, we design an instantaneous channel gain mapping based polarization scheme for increasing the randomness of the secret key, hence enhancing the overall system performance, as detailed bellow.

The key innovations of this scheme are boldly contrasted to the state-of-the-art in Table I, which are further detailed as follows:

- We propose a novel PLS architecture based on a MIMO scheme, modulation, and multi-domain polarization. This scheme integrates the multi-domain polarization structure with the classic binary polarization coding structure for enhancing the overall system's polarization effect, to a benefit, our solution achieves significant performance improvements over conventional MIMO transmissions. Exploiting the randomness of the MIMO detection order as our secret physical layer key, distinct polarization designs are derived based on different detection orders, yielding unique coding constructions. Since E cannot infer the legitimate link's detection order, it also fails to acquire the corresponding coding construction. This approach enhances the legitimate link's decoding performance and simultaneously it degrades the E link's quality, hence improving the security.
- We conceive an instantaneous channel gain based mapping and coding structure. To further enhance the PLS, this method partitions the legitimate link's instantaneous gain into multiple contiguous but non-overlapping intervals, each mapping to a distinct coding construction. By employing the Gaussian approximation (GA) algorithm to match the subchannel reliability, which uses the noise variance of the channel as input to select the most reliable bits, the secret key may be obtained without incurring any additional overhead. Even if E has powerful computational capabilities, it fails to perform accurate decoding. Again, partitioning the legitimate link's gain improves the legitimate link's error correction capability, while degrading the decoding capability of E.
- To validate the proposed scheme's confidentiality in the presence of eavesdroppers, we analyze the maximum

achievable secrecy rate from various perspectives. Our numerical results confirm the scheme's confidentiality. Furthermore, we evaluate the performance of this approach in terms of both its bit error rate (BER) and block error rate (BLER). Our simulation results demonstrate that even in possession of formidable computing power, eavesdroppers cannot correctly decode a complete data frame. For example, within a 4×4 MIMO configuration, the proposed PLS approach attains an SNR enhancement of 2dB in comparison to conventional MIMO, while the eavesdropper's BLER approaches 100% and the legitimate user's BLER is as low as 10^{-5}.

The rest of this paper is composed as follows. In Section II, we portray the system model and provide a detailed description of the key generation scheme relying on MIMO based multi-domain polarization. Section III presents the receiver models of both the legitimate user and of the eavesdropper. Subsequently, in Section IV, we analyze the system's secrecy rate. Section V provides our simulation results and theoretical analysis. Finally, Section VI concludes of the paper.

As for our notations, random variables and their actual values are represented by uppercase Roman letters and lowercase letters, respectively. Furthermore, $\Re(x)$ and $\Im(x)$ represent the real and imaginary parts of x, respectively. The modulus of x is written as $\|x\| = \sqrt{\Re(x)^2 + \Im(x)^2}$. The calligraphic characters $\mathcal{X}$ and $\mathcal{Y}$ are used to denote sets, and $|\mathcal{X}|$ denotes the number of elements in $\mathcal{X}$. The notation $P(X)$ represents the probability density function (PDF) of random variables, and the probability density function of X is expressed as $p(X|A)$ under the condition of a given A. In addition, $\Gamma(n)$ represents the gamma distribution having n degrees of freedom. Matrices and vectors are represented by bold uppercase and lowercase letters, respectively. In particular, $\mathbf{0}_{N\times1}$ denotes the $(N\times1)$ zero vector and $\mathbf{I}_N$ denotes the $(N\times N)$ identity matrix. The transpose and conjugate transpose operators are denoted by $(\cdot)'$ and $(\cdot)^\dagger$, respectively. Moreover, the element in the i-th row and the j-th column of matrix $\mathbf{H}$ is written as $h_{i,j}$, while $\mathbf{x}_1^N$ represents the vector $(x_1, x_2, ..., x_N)'$. Finally, we employ the notation $E(\cdot)$ to represent the mean operator, and $\|\cdot\|_F$ denotes the two-norm operation.

II. PLS design for Multi-domain polarisation MIMO system

This section elaborates on our PLS framework, which relies on MIMO based multi-domain polarization.

A. Channel Model

Consider the MIMO wiretap channel model depicted in Fig. 1. Given a total of S time slots (TS), the transmitter (Alice) sends K information bits to the legitimate user (Bob) after polar coding, interleaving, and modulation using a coding rate of $R = K/N$, where N is the code length. An eavesdropper attempts to intercept the confidential information transmitted via the legitimate link. Alice is equipped with T_A transmit antennas (TAs), while Bob and Eve have N_B and N_E receive antennas (RAs), respectively. The uncorrelated Rayleigh fading channels encountered by the legitimate link and the eavesdropping link are denoted by $\mathbf{H} = [\mathbf{h_1}, \mathbf{h_2}, \cdots, \mathbf{h}_{\mathrm{T_A}}]$ and $\mathbf{G} = [\mathbf{g_1}, \mathbf{g_2}, \cdots, \mathbf{g}_{\mathrm{T_A}}]$, which have sizes of $(N_B \times T_A)$ and $(N_E \times T_A)$, respectively. Each column vector in the matrices $\mathbf{H}$ and $\mathbf{G}$ is expressed as $\mathbf{h}_\mathrm{t} = [\mathrm{h}_{1,\mathrm{t}}, \mathrm{h}_{2,\mathrm{t}}, \cdots, \mathrm{h}_{\mathrm{N_B,t}}]'$ and $\mathbf{g}_\mathrm{t} = [\mathrm{g}_{1,\mathrm{t}}, \mathrm{g}_{2,\mathrm{t}}, \cdots, \mathrm{g}_{\mathrm{N_E,t}}]'$, where $t = 1, 2, ..., T_A$, respectively. The vectors $\mathbf{h}_\mathrm{t}$ and $\mathbf{g}_\mathrm{t}$ include the channel coefficients of the link spanning from Alice's t-th TA to all RAs of Bob and Eve. Additionally, for any TS, all channel coefficients $\mathrm{h}_{b,t}$ and $\mathrm{g}_{e,t}$ obey $\mathcal{CN}(0,1)$, where b and e represent the b-th row and e-th row of $\mathbf{H}$ and $\mathbf{G}$, respectively, while t represents the t-th column of $\mathbf{H}$ and $\mathbf{G}$, respectively, with $b = 1, 2, ..., N_B, e = 1, 2, ..., N_E$.

In a Time Division Duplex (TDD) system, the channel's reciprocity may be exploited without additional resources or overhead, ensuring that Alice and Bob have similar channel coefficients at both end of the link. Therefore, in any TS s, the received signal expressions for Bob and Eve are given by:

$$\mathbf{y}_1^{N_B}(s) = \mathbf{H}(s) \cdot \mathbf{x}_1^{T_A}(s) + \mathbf{z}_1^{N_B}(s), \tag{1}$$

$$\mathbf{y}_1^{N_E}(s) = \mathbf{G}(s) \cdot \mathbf{x}_1^{T_A}(s) + \mathbf{z}_1^{N_E}(s). \tag{2}$$

In the s-th TS, $s = 1, 2, ..., S$, the vector $\mathbf{y}_1^{NB}(s)$ of size $(N_B \times 1)$ represents Bob's received signal, and the vector $\mathbf{y}_1^{NE}(s)$ of size $(N_E \times 1)$ contains Eve's received signal. The $(T_A \times 1)$ vector $\mathbf{x}_1^{TA}(s)$ represents the symbol transmitted by Alice. Furthermore, the $(N_B \times 1)$ vector $\mathbf{z}_1^{N_B}(s)$ and the $(N_E \times 1)$ vector $\mathbf{z}_1^{N_E}(s)$ obey the complex Gaussian distributions $\mathcal{CN}\left(\mathbf{0}_{N_B\times1}, \sigma^2\mathbf{I}_{N_B}\right)$ and $\mathcal{CN}\left(\mathbf{0}_{N_E\times1}, \sigma^2\mathbf{I}_{N_E}\right)$, containing Bob's and Eve's additive white Gaussian noise (AWGN) components, respectively.

B. Key generation based on multi-domain polarization

Building on the concept of generalized polarization, we aim for enhancing the MIMO transmission efficacy and hence the overall system performance by jointly optimizing the coding and MIMO transmission [35]. Again, we propose a MIMO based multi-domain polarization architecture that improves the error correction capability of the legitimate link, while degrading the eavesdropping link's performance. As depicted in Fig. 2, the scheme comprises three primary stages [35]. In the first stage, MIMO polarization is carried out, which defined as partitioning the original MIMO channel into multiple parallel sub-channels. In the second stage, modulation polarization is carried out following the multi-level coding concept [36, 37] to generate additional bit-based subchannels. Finally, the time slot index is introduced to maximize the system's polarization effect and to select the most reliable bit subchannel for information transmission. Moreover, for avoiding the practical challenges of obtaining the complete legitimate link's CSI, we utilize only the channel's instantaneous gain to design the secure system based on this multi-level polarization approach.

We define the original MIMO channel as $\mathbf{W} : \mathcal{X}^{T_A} \mapsto \mathcal{Y}$, where $\mathcal{X}^{T_A}$ represents the set of transmitted symbols for each antenna and $|\mathcal{X}^{T_A}| = M$, with M being the modulation order, while $\mathcal{Y}$ represents the set of received signals. In TDD systems, the legitimate link's instantaneous channel gain is estimated by the legitimate party. Under such circumstances,

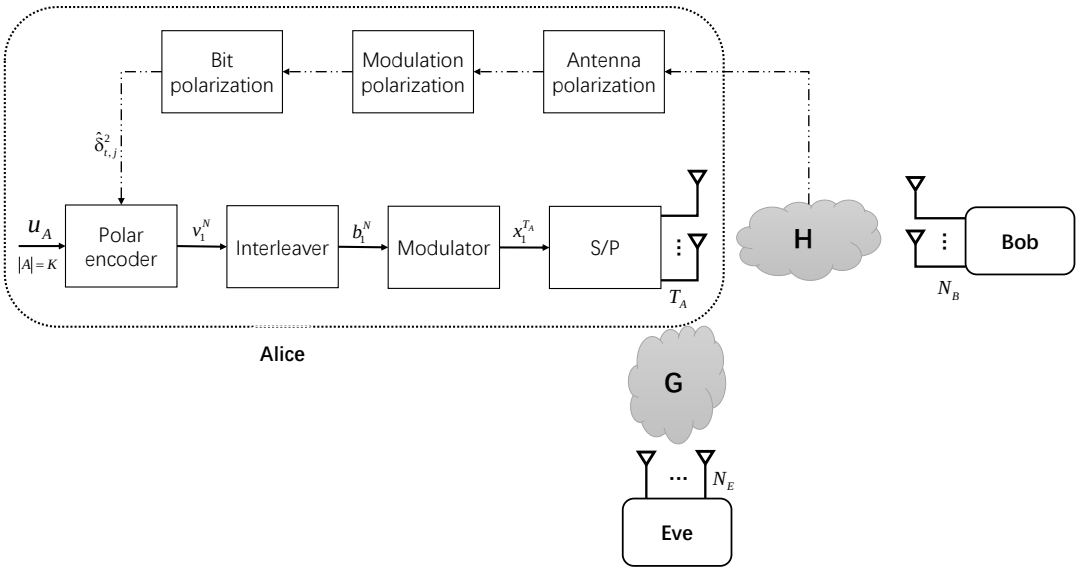


Fig. 1: Physical layer security scheme based on MIMO multi-domain polarization.

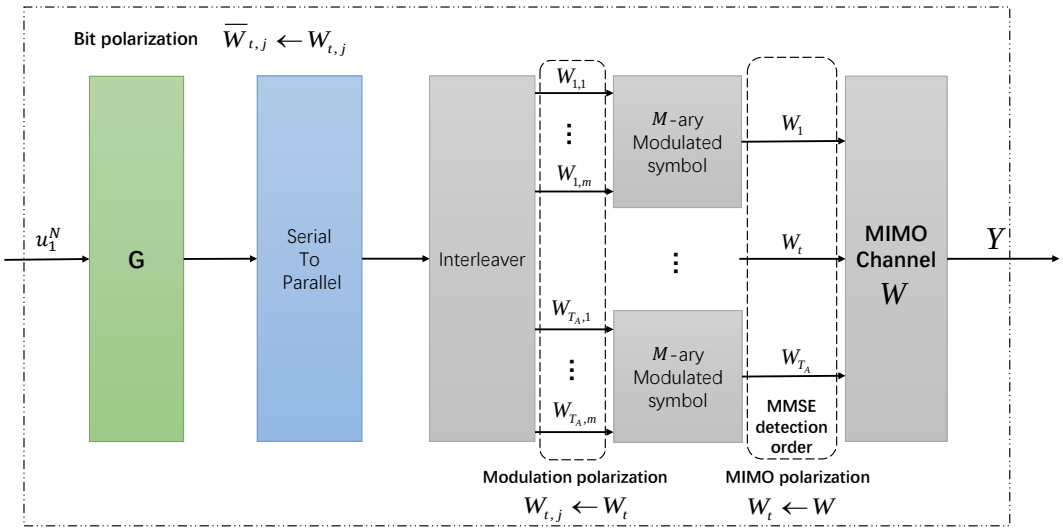


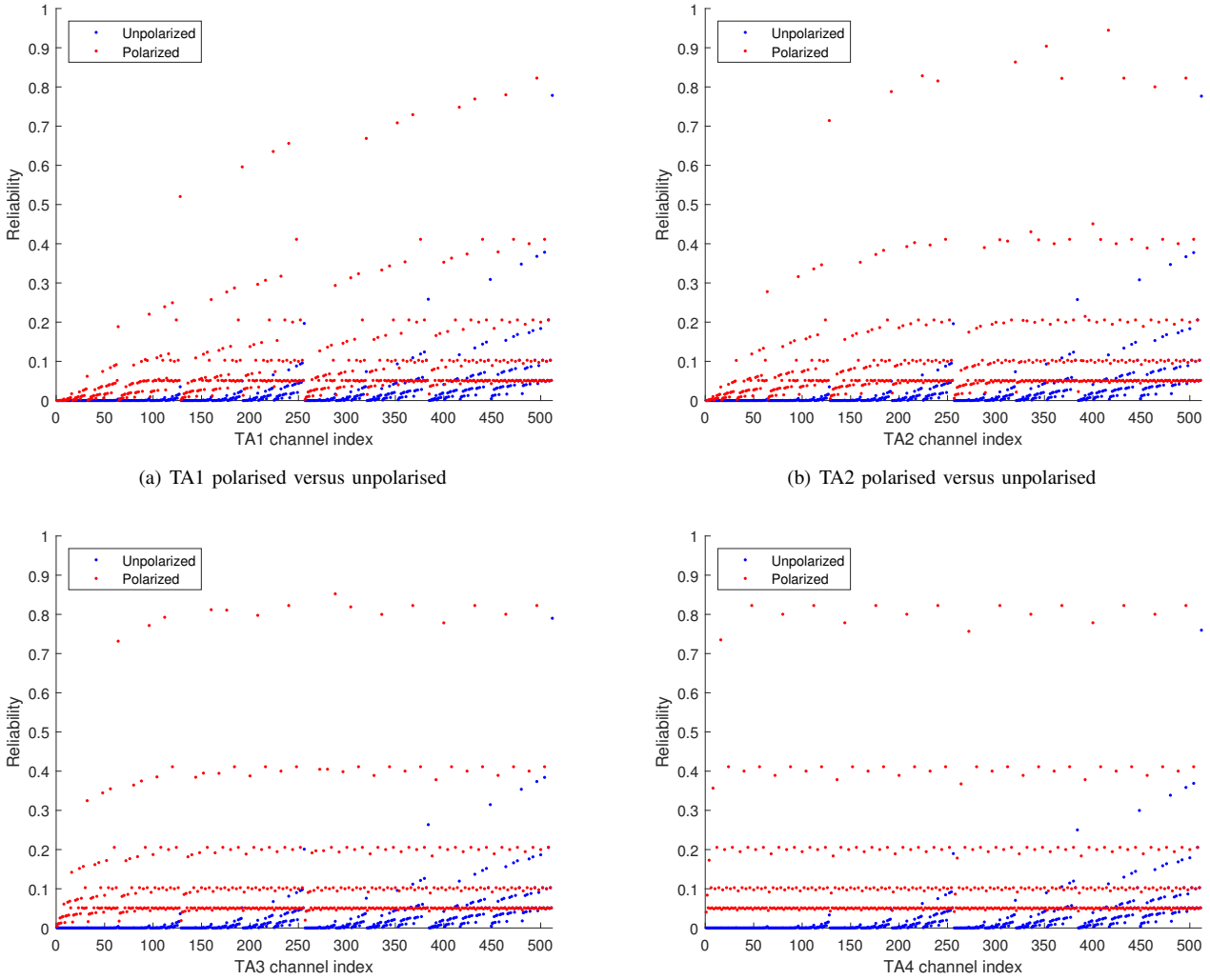
Fig. 2: Architecture of MIMO based polarisation at the transmitter.

the transition probability $\mathbf{W}\left(\mathbf{y}_1^{N_B}(s) \mid \mathbf{x}_1^{T_A}(s), \mathbf{H}(s)\right)$ of the legitimate link can be derived according to equation (1), which can be expressed in the s-th TS as [35]:

$$\mathbf{W}\left(\mathbf{y}_1^{N_B}(s) \mid \mathbf{x}_1^{T_A}(s), \mathbf{H}(s)\right) = \left(\pi\sigma^2\right)^{-N_B} \cdot \exp\left(-\sum_{i=1}^{N_B} \frac{\|y_i - \tilde{x}_i\|^2}{\sigma^2}\right), \tag{3}$$

where $\tilde{x}_i$ is the i-th element of the $(N_B \times 1)$ vector $\tilde{\mathbf{x}}_s^{N_B}(s) = \mathbf{H}(s) \cdot \mathbf{x}_1^{T_A}(s), i = 1, 2, \ldots, N_B,\ s = 1, 2, ..., S$, while y_i is the i-th element of the $(N_B \times 1)$ vector $\mathbf{y}_1^{N_B}(s)$, and σ^2 denotes the noise variance.

At this stage, we perform MIMO polarization. Since the MIMO detection scheme has varying detection orders for each spatial layer, which results in different signal reliability across the individual antennas. For instance, under the linear minimum mean square error (MMSE) successive interference cancellation (SIC) algorithm, the first detected antenna has relatively low reliability due to the interference imposed by the other antennas. Provided that the corresponding symbol was still detected without error, the detected symbol is remodulated and then subtracted both the composite signal, This way the interference is gradually peeled off, thence typically the last detected antenna has the highest reliability due to the absence of interference, which was cancelled by subtracting the remodulated signals of all other RAs. As illustrated in Fig. 3, an incremental detection pattern was used in the detection process. In the figure we can see a comparison of the reliability of the different antennas both before and after polarisation. The results show that the average reliability of



(a) TA1 polarised versus unpolarised

(b) TA2 polarised versus unpolarised

(c) TA3 polarised versus unpolarised

(d) TA4 polarised versus unpolarised

Fig. 3: Examples of 4×4 MIMO antenna polarisation.

the antennas after polarisation is significantly higher, further validating the effectiveness of the polarisation technique used. In addition, it should be noted that in the incremental detection mode, the average reliability of the antennas detected in the reverse scan exceeds that of the antennas in the forward scan. This confirms the conclusion of the previous analysis, namely that the interference imposed on the last detected antenna is completely removed. Under this condition, the original MIMO scheme is divided into T_A independent sub-channels $\mathbf{W} \rightarrow \mathbf{W}_t : \mathcal{X} \mapsto \mathcal{Y}, t = 1, 2, \ldots, T_A$, each associated with different symbol reliability, where $\mathcal{X}$ denotes the set of transmitted symbols. The associated transition probabilities can be further expressed as:

$$\mathbf{W}_t\left(\mathbf{y}_1^{N_B}(s) \mid x_t, \mathbf{H}(s)\right) = \sum_{\mathbf{x}_1^{T_A}(s)\backslash x_t} \frac{1}{2^{m(T_A-1)}} \cdot \mathbf{W}\left(\mathbf{y}_1^{N_B}(s) \mid \mathbf{x}_1^{T_A}(s), \mathbf{H}(s)\right), \tag{4}$$

where $m = \log_2^M$ represents the number of bits per M-ary quadrature amplitude modulation (QAM) symbol, and $\mathbf{x}_1^{T_A}(s)\backslash x_t$ denotes the subvector of $\mathbf{x}_1^{TA}(s)$, excluding element x_t at the s-th TS.

After obtaining T_A independent sub-channels having different symbol reliability levels, we proceed to perform modulation polarization [37], introducing polarization effects into the modulated symbol so that each bit sub-channel constituted for example the first or the last bit of the symbol exhibits varying reliability $\mathbf{W} \rightarrow \mathbf{W}_t \rightarrow \mathbf{W}_{t,j} : \mathcal{B} \mapsto \mathcal{X} \mapsto \mathcal{Y}, t = 1, 2, \ldots, T_A, j = 1, 2, ...m$, where $\mathcal{B}$ represents the set of transmitted bits $b_{t,j}$. At this point, the transition probability can be written as:

$$\begin{aligned}
&\mathbf{W}_{t,j}\left(\mathbf{y}_1^{N_B}(s) \mid b_{(t-1)m+j}, \mathbf{H}(s)\right) \\
&= \sum_{\mathbf{b}_{(t-1)m+j}^{tm}\backslash b_{(t-1)m+j}} \left(\frac{1}{2^{m-1}} \cdot \mathbf{W}_t\left(\mathbf{y}_1^{N_B}(s) \mid x_t, \mathbf{H}(s)\right)\right) \\
&= \sum_{\mathbf{b}_{(t-1)m+j}^{tm}\backslash b_{(t-1)m+j}, \mathbf{x}_1^{T_A}(s)\backslash x_t} \left(\frac{1}{2^{T_A N_B - 1}} \cdot \mathbf{W}\left(\mathbf{y}_1^{N_B}(s) \mid \mathbf{x}_1^{T_A}(s), \mathbf{H}(s)\right)\right),
\end{aligned} \tag{5}$$

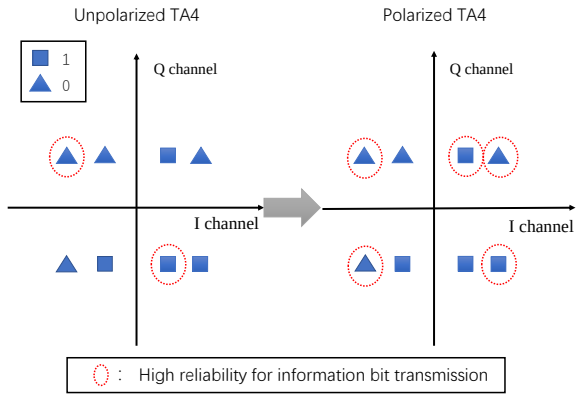


Fig. 4: Examples of bit polarisation of the last antenna detected in increasing order within a 4×4 MIMO scheme where QPSK is used.

where $\mathbf{b}^{m}_{(t-1)m+j}\backslash b_{(t-1)m+j}$ represents the bit subvector $\mathbf{b}^{m}_{(t-1)m+j}$ excluding the element $b_{(t-1)m+j}$. Then the binary vector $\mathbf{b}^{tm}_{(t-1)m+j}$ is mapped to the M-ary transmitted symbol x_t according to the modulation order M.

Lastly, we incorporate the time index. Given that the total number of TSs is S, the original information sequence is mapped to the corresponding bit sub-channel using polarization coding to state N independent bit sub-channels $\mathbf{W} \rightarrow \mathbf{W}_t \rightarrow \mathbf{W}_{t,j} \rightarrow \overline{\mathbf{W}}_{t,j} : \mathcal{U} \mapsto \mathcal{B} \mapsto \mathcal{X} \mapsto \mathcal{Y}$, where $\mathcal{U}$ represents the set of original information bits $u_{t,j}$ having a cardinality of $|\mathcal{U}| = K$. The transition probability can then be expressed as:

$$\overline{\mathbf{W}}_{t,j}\left(\mathbf{Y}_B, \mathbf{u}_1^{n-1} \mid u_n\right) = \sum_{\mathbf{u}_{n+1}^{N}, \mathbf{b}^{tm}_{(t-1)m+j}\backslash b_{(t-1)m+j}} \frac{\prod_{s=1}^{S} \mathbf{W}_{t,j}\left(\mathbf{y}_1^{N_B}(s) \mid b_{(t-1)m+j}, \mathbf{H}(s)\right)}{2^{N-1}}. \quad (6)$$

Upon employing the above three-level polarization based channel transformation, the original MIMO channel is polarized into N binary memoryless channels (BMCs). Our MIMO based multi-domain polarization design relies on this cascading principle. The most reliable antenna is selected first through antenna polarization, followed by the selection of the most reliable bit from each RA's modulated symbol. Ultimately, the information bits having the highest reliability are matched across all TSs, resulting in the final polar coding structure. As a benefit of its iterative application [38], the MMSE detection algorithm is used for generating the physical layer key, which is used for mapping the different coding constructs to different antenna detection sequences. In Fig. 4, a toy example is presented to compare the reliability of the antenna that was detected last after polarisation to its unpolarised state, when considering detection executed in ascending order. The figure shows a constellation diagram for QPSK modulation with 8 points forming 4 different QPSK symbols. In the unpolarised case, only a limited number of reliable bits can be obtained in the transmitted symbols, the rest being known as frozen bits. However, after polarisation, more reliable bits can be obtained under the same conditions. The reason for this is that after polarisation the average reliability of the bit sub-channel is increased, especially for the symbols transmitted by the last detected antenna, which suffers the least interference. This leads to a significant alteration in the pattern of the polarisation coding structure.

Based on Equations (1) and (4), the MMSE detector acquires soft estimates of T_A independent data streams in the s-th TS, after the legitimate party receives the signal associated with the known instantaneous gain of the legitimate link. In this case, the eavesdropper is unable to infer the specific polarization pattern and coding structures since the specific detection method is unattainable. Following the increasing detection order, the soft estimate [39] of the t-th data stream is formulated as:

$$\gamma_t(s) = \sum_{\xi=1}^{N_B} w^t_{1,\xi}(s)\tilde{y}_\xi(s), \quad (7)$$

where $\tilde{y}_\xi(s)$ represents the ξ-th element of the error vector $\tilde{\mathbf{y}}_1^{N_B}(s) \triangleq \mathbf{y}_1^{N_B}(s) - \sum_{\tilde{t}=1}^{t-1} \mathbf{H}_{\tilde{t}}(s)\hat{x}_{\tilde{t}}$ of the received signal in s-th time slot. $\mathbf{H}_{\tilde{t}}(s)$ represents a fraction of the original MIMO matrix $\mathbf{H}(s)$ scanning him first column to the $\tilde{t}$-th column, while $\hat{x}_{\tilde{t}}$ represents the symbolic estimate of the $\tilde{t}$-th data stream. Moreover, $w^t_{1,\xi}(s)$ represents the ξ-th element in the first row of $\mathbf{W}^t(s)$, which is the MMSE detection matrix for the t-th data stream and its expression is as follows [38] :

$$\mathbf{W}^t(s) = \left(\left(\mathbf{H}^t(s)\right)^\dagger \mathbf{H}^t(s) + \sigma^2 \mathbf{I}_{T_A-t+1}\right)^{-1} \left(\mathbf{H}^t(s)\right)^\dagger, \quad (8)$$

where the matrix $\mathbf{H}^t(s)$ represents a fraction of $\mathbf{H}(s)$ scanning him t-th column to the T_A-th column and $\mathbf{I}_{T_A-t+1}$ is a unit matrix of size $T_A - t + 1$.

Considering that the MMSE detection order is random and the transmitter is equipped with T_A antennas, the legitimate link will possess $T_A!$ distinct detection modes, resulting in $T_A!$ unique coding structures for the legitimate link. Under various detection modes, we introduce the equivalent AWGN channel $\widetilde{\mathbf{W}}_{t,j}$ for transmission. The bit subchannel noise variance, which is obtained under a specific channel fading condition, is transformed into the effective noise variance under the AWGN channel, allowing the same error performance to be achieved under both channels. This implies that the average mutual information (AMI) of the equivalent AWGN channel and the polarized bit subchannel are identical, yielding:

$$I\left(\overline{\mathbf{W}}_{t,j}\right) = I\left(\widetilde{\mathbf{W}}_{t,j}\right). \quad (9)$$

Given the noise variance σ^2, the expression can be written as [35]:

$$I_{\overline{\mathbf{W}}_{t,j}}(\sigma) = I_{\widetilde{\mathbf{W}}_{t,j}}(\sigma_{t,j}) = \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} p(y_B)\log_2[p(y_B)]dudv - 0.5\log_2\left(2\pi e\sigma^2_{t,j}\right), \quad (10)$$

where y_B denotes the signal received by the legitimate users, and $u = \Re\left(\mathrm{y}_B\right), v = \Im\left(\mathrm{y}_B\right)$.

In the end, the equivalent noise variance $\sigma^2_{t,j}$ of each bit subchannel is utilized to employ a Gaussian approximation (GA)

algorithm for matching the reliability of each sub-channel, as illustrated in Algorithm 1. Subsequently, confidential information is transmitted with the aid of polarization coding. The distinct detection sequences of the MIMO polarization result in varying antenna reliability levels, leading to different equivalent AWGN variances and coding methods due to the chain reaction of modulation polarization and bit polarization. Again, the random detection order of MIMO polarization determines the secret physical layer key, which is shared by the legitimate link. By contrast, the eavesdropper has only a $1/T_A!$ chance of obtaining the correct key. Even if E tentatively tries all possible detection orders, it still cannot determine the correct decoding result. The reason for this is that the detection order determined only ranks the reliability of the antenna and does not give a specific coding structure, which substantially increases the error probability of E. This approach significantly enhances the performance of the legitimate link with the aid of our specific MIMO polarization design, but also considerably degrades the decoding performance of the eavesdropper.

C. Channel gain segmentation design

The MIMO polarization scheme of the previous subsection exhibited confidentiality limitations when the number of TAs is small. Consequently, we further explore potential methods of enhancing the system's confidentiality. As a benefit of the reciprocity of TDD systems, both parties have similar instantaneous gain values; however, the eavesdropper cannot obtain the legitimate link's instantaneous gain. Building on this concept, we model the gain $\mu_{\mathrm{t}} = \mathbf{h}_{\mathrm{t}}^{+}\mathbf{h}_{\mathrm{t}}$ of all RAs corresponding to the transmitter's t-th antenna and partition it into P contiguous, but non-overlapping sub-intervals. In the Rayleigh fading channel model, the probability distribution function (PDF) of the gain μ for each TA can be expressed as:

$$p(\mu) = \frac{1}{2^{T_A}\Gamma(T_A)} x^{T_A-1} e^{-\mu/2}, \tag{11}$$

where the Gamma function is $\Gamma(T_A) = \int_0^{+\infty} \tau^{T_A-1} e^{-\tau} \mathrm{d}\tau$.

Integrating the above equation yields P continuous subintervals :

$$\int_{\alpha_{p-1}}^{\alpha_p} \frac{1}{2^{T_A}\Gamma(T_A)} \mu^{T_A-1} e^{-\mu/2} d\mu = 1/P. \tag{12}$$

Upon incorporating the channel gain segments into our MIMO polarization design, the different channel gain intervals map to distinct equivalent variances during the MIMO polarization process, subsequently yielding different coding methods, when matching the sub-channel reliability utilizing the classic GA algorithm, as outlined in Algorithm 1. Moreover, the transmitter has P unique coding methods for an identical detection order pattern. Table II exemplifies the coding patterns for each sub-channel, when we have $P = 16$ and a code length of $N = 32$.

The segmentation of channel gain not only compensates for the constraints of the MIMO polarization design scheme, but it even enhances the system's security. Under different detection sequences, distinct gain modes yield $T_A! \times P$ disparate coding schemes. However, the eavesdropper is unable to ascertain the detection sequence mode during the MIMO polarization process, nor can it obtain the legitimate link's instantaneous gain. Consequently, even if the eavesdropper acquires confidential information, it remain unaware of the correct coding structure, and thus, cannot achieve accurate decoding results.

Algorithm 1 Generation of Coding Construction Scheme $\mathbf{u}_{\mathcal{F}}^{(p)}$

Require:
Code length N
Number of transmitting antennas T_A
Modulation order M
Number of channel interval P
Channel gain $\mu_t, t = 1, 2, ...T_A$
Equivalent AWGN noise variance $\delta_{t,j}^2$
Length of information bits K
Ensure:
Frozen bit pattern $\mathbf{u}_{\mathcal{F}}^{(p)}$
for $1 \le t \le T_A$ **do**
  Calculate P different channel intervals $\left[\varphi_{t,p-1}, \varphi_{t,p}\right)$ for t-th antenna according to (12);
  Obtain $\left[\phi_{t,p-1}, \phi_{t,p}\right)$ by matching the channel interval with μ_t;
  for $1 \le j \le log2^M$ **do**
    Calculate initial $\alpha_{t,j} = \left(\left(\frac{1}{\delta_{t,j}^2}\right) \cdot \left(\frac{\phi_{t,p-1}+\phi_{t,p}}{2}\right)\right)^{-\frac{1}{2}}$;
    Initialize the LLR mean value of the MIMO channel $\mathbf{W}$ $m_{t,j}^{(1)} = \frac{2}{\alpha_{t,j}^2}$;
    for $0 \le l \le n-1$ **do**
      Calculate the mean LLR $m_{t,2^n}^{(i)}$ of the subchannel iteratively according to [38];
      for $1 \le i \le 2^j$ **do**
        $m_{t,2^{j+1}}^{(2i-1)} = \phi^{-1}\left[1 - \left(1 - \phi\left(m_{t,2^j}^{(i)}\right)\right)^2\right]$;
        $m_{t,2^{j+1}}^{(2i)} = 2m_{t,2^j}^{(i)}$;
      end for
    end for
  end for
end for
Sort $m_{t,2^n}^{(i)}$ from smallest to largest;
$\mathbf{u}_{\mathcal{F}}^{(p)}$ takes the first $N-K$ values of $m_{t,2^n}^{(i)}$

III. Receiver Design

In this section, a detailed description of our receiver design employing MIMO polarization techniques is provided, along with an exposition of the processing steps for both the legitimate and eavesdropping parties.

A. Legitimate receiver

For the legitimate user, a shared physical layer key exists for communication with the transmitter, enabling the acquisition of accurate MIMO detection sequence patterns and channel gain segmentation patterns. To minimize the processing latency and enhance the receiver performance attained, the legitimate receiver utilizes a minimum mean square error (MMSE) algorithm for concatenated MIMO detection and

TABLE II: Coding pattern for $P = 16$ and $N = 32$

P	Channel Gain Interval	Code Patterns
1	[0,1.4746)	1755
2	[1.4746,1.8982)	5555
3	[1.8982,2.2346)	5754
4	[2.2346,2.5353)	115F
5	[2.5353,2.8199)	017F
6	[2.8199,3.0993)	1577
7	[3.0993,3.3811)	107F
8	[3.3811,3.6721)	5457
9	[3.6721,3.9795)	1755
10	[3.9795,4.3132)	3355
11	[4.3132,4.6823)	1557
12	[4.6823,5.1096)	5353
13	[5.1096,5.6293)	70F1
14	[5.6293,6.3184)	FF00
15	[6.3184,7.4166)	01F7
16	[7.4166, +∞)	017F

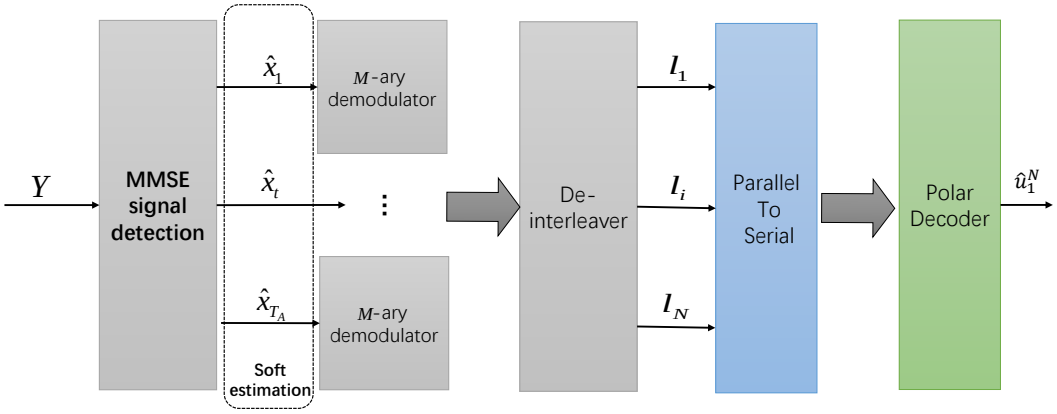


Fig. 5: Architecture based on our MIMO polarisation design at the receiver.

decoding. The MIMO detection's soft estimate is forwarded to the demodulator to derive the log-likelihood ratio (LLR), which is subsequently sent to the decoder for a hard decision, as illustrated in Fig. 5. The LLR expression is as follows [30]:

$$\mathrm{LLR_B}\left(b_{t,j}\right) = \ln \frac{\sum_{b_{t,j}=0} \exp\left(-\frac{\left\|\mathbf{y_B}(b_{t,j})-[\mathbf{h}_1 \cdots \mathbf{h}_{N_B}]\mathbf{x}(b_{t,j})\right\|_{\mathrm{F}}^2}{\sigma_B^2}\right)}{\sum_{b_{t,j}=1} \exp\left(-\frac{\left\|\mathbf{y_B}(b_{t,j})-[\mathbf{h}_1 \cdots \mathbf{h}_{N_B}]\mathbf{x}(b_{t,j})\right\|_{\mathrm{F}}^2}{\sigma_B^2}\right)}, \quad (13)$$

where $\mathbf{y_B}(b_{t,j})$ represents the signal received by the legitimate receiver, while $\mathbf{x}(b_{t,j})$ denotes the modulation symbol comprising the transmitted bits $b_{t,j}$, and σ_B^2 is the noise variance of the legitimate link.

The LLRs are derived based on equation (13) and subsequently they are input into the successive cancellation (SC) based stack polar decoder [39] for making hard decisions, as depicted in Fig 6.

Initially, the SC decoder carries out the operation seen in Fig 6(a), executing the f function to the $(j+1)$-st layer using the i-th and $(i+2^{j-1})$-th LLRs on the left to obtain a new LLR, $l_i^{(j)}$. This can be expressed as:

$$\begin{aligned} l_i^{(j)} &= f\left(l_i^{(j+1)}, l_{i+2^{j-1}}^{(j+1)}\right) \\ &= 2\tanh^{-1}\left(\tanh\left(l_i^{(j+1)}/2\right)\tanh\left(l_{i+2^{j-1}}^{(j+1)}/2\right)\right) \\ &\approx \mathrm{sign}\left(l_i^{(j+1)}\right)\mathrm{sign}\left(l_{i+2^{j-1}}^{(j+1)}\right)\min\left(\left|l_i^{(j+1)}\right|, \left|l_{i+2^{j-1}}^{(j+1)}\right|\right) \end{aligned} \quad (14)$$

The new LLR, $l_i^{(j)}$, is then subjected to hard decisions based on the coding structure of the legitimate link, which can be formulated as:

$$\hat{u}_i = \begin{cases} 0 & \text{if } l_i^{(1)} \geq 0 \text{ or frozen bit} \\ 1 & \text{otherwise} \end{cases} \quad (15)$$

Once the hard-decision based value of the i-th bit is determined, the LLRs $l_i^{(j+1)}$ and $l_{i+2^{j-1}}^{(j+1)}$ of the $(j+1)$-st layer are combined for executing the g function, subsequently acquiring the soft information for the next bit. This is expressed as:

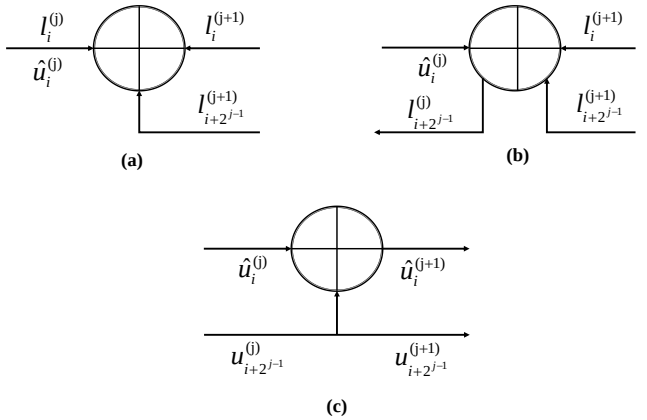


Fig. 6: . The SC decoding process for the mod-2 sum of the i-th and the $(i+2^{j-1})$-th bits at the j-th level: (a) the f function, (b) the g function and (c) partial sum calculation.

$$l_{i+2^{j-1}}^{(j)} = \begin{cases} l_{i+2^j}^{(j+1)} + x_i^{(j+1)} & \text{if } \hat{u}_i^{(j)} = 0 \\ l_{i+2^{(j-1)}}^{(j+1)} - x_i^{(j+1)} & \text{otherwise .} \end{cases} \tag{16}$$

Likewise, the hard decision in Equation (15) is executed based on the encoding structure of the legitimate link. Following this, $\hat{\mu}_i^{(j)}$ and $\hat{\mu}_{i+2^{j-1}}^{(j)}$ undergo XOR processing to derive $\hat{\mu}_i^{(j+1)}$, while $\hat{\mu}_{i+2^{j-1}}^{(j)}$ is directly transferred to $\hat{\mu}_{i+2^{j-1}}^{(j+1)}$. By iteratively performing the three operations depicted in Fig. 6, hard decisions are obtained for all transmitted bits, resulting in the final decoding outcome.

Furthermore, to enhance the decoding capability of the legitimate link, the so-called successive cancellation list (SCL) and cyclic redundancy check (CRC)-SCL decoding algorithms of [40] can be employed, which offer superior performance.

As for the receiver design, the detector and decoder rely on a serial by concatenate construction. The computational overhead of the MMSE algorithm mainly depends on the dimension of the channel matrix and on the implementation of the algorithm, with a complexity order of $O[(T_A^2)]$ per symbol, where T_A is the number of transmit antennas. Subsequently, the soft information representing the data is fed to the polarisation decoder, and the complexity of the SC decoder depends both on the number of iterations as well as on the dimensionality of the input data, which in our scheme has a complexity of $O[(\log(T_A))]$ per symbol. Specifically, the complexity per symbol in the proposed scheme may reach $O[(T_A^2 * \log(T_A))]$.

The main reason for adopting the cascaded structure based on MMSE detection and SC decoding is that this receiver has both a low computational complexity as well as delay, which is favourable for employment in practical systems. In large-scale MIMO systems, this low-complexity and low-latency implementation is of pivotal significance.

B. Eavesdropper

As for the eavesdropper, an identical MMSE detection algorithm is employed for performing soft estimation of the intercepted signal. This is then entered into the demodulator to derive the soft LLRs, which can be expressed as:

$$\mathrm{LLR_E}\left(b_{t,j}\right) = \ln \frac{\sum_{b_{t,j}=0} \exp\left(-\frac{\left\|\mathbf{y_E}(b_{t,j}) - [\mathbf{g}_1 \cdots \mathbf{g}_{N_E}]\mathbf{x}(b_{t,j})\right\|_{\mathrm{F}}^2}{\sigma_E^2}\right)}{\sum_{b_{t,j}=1} \exp\left(-\frac{\left\|\mathbf{y_E}(b_{t,j}) - [\mathbf{g}_1 \cdots \mathbf{g}_{N_E}]\mathbf{x}(b_{t,j})\right\|_{\mathrm{F}}^2}{\sigma_E^2}\right)}, \tag{17}$$

where $\mathbf{y}_{\mathrm{E}}(b_{t,j})$ represents the signal received by the eavesdropper, Eve, while $\mathbf{x}(b_{t,j})$ represents the modulation symbol comprising the transmitted bits $b_{t,j}$ and σ_E^2 is the noise variance of Eve's link.

Subsequently, these LLRs are fed into the decoder for error correction. On one hand, Eve is incapable of obtaining the antenna detection sequence pattern during the MIMO polarization of the legitimate link. She only has a $1/TA!$ probability of acquiring the correct detection pattern, which prevents her from inferring the variance of the equivalent fading channel or the coding structure of the legitimate link. On the other hand, even when the transmitter has a limited number of antennas, the eavesdropper is unable to determine the channel gain range of the legitimate link, which also prevents her from acquiring the coding structure of the legitimate link. The PLS framework, based on our MIMO polarization design combined with the channel gain segmentation based design, enhances the performance of the legitimate link, while significantly degrading the eavesdropper's success probability.

IV. Secrecy rate analysis

In this section, the secrecy rate for the proposed scheme is analyzed under both Gaussian-distributed input and finite-alphabet input scenarios. The secrecy rate is defined as the positive difference between the maximum achievable data rates of the legitimate and eavesdropping links.

A. Gaussian-distributed input

Under the Gaussian-distributed input condition, it is assumed that the signal transmitted by the legitimate link obeys the complex Gaussian distribution $\mathcal{CN}\left(0, \sigma_B^2\right)$. Based on the above secrecy rate definition, the secrecy rate under the Gaussian-distributed input condition is formulated as:

$$I_{PLS} = \max\left\{0, I\left(\mathbf{W}_B\right) - I\left(\mathbf{W}_E\right)\right\}, \tag{18}$$

where $I(\mathbf{W}_B)$ and $I(\mathbf{W}_E)$ denote the channel capacities of the legitimate and eavesdropping links, respectively.

Since the instantaneous gain of the channel is discretised, the channel capacities of the legitimate and eavesdropping links under Gaussian-distributed input conditions can be further expressed as:

$$I\left(\mathbf{W}_B\right) = \frac{1}{P} \cdot \sum_{p=1}^{P} I\left(\mathbf{W}_B\right)^{(p)}, \tag{19}$$

$$I\left(\mathbf{W}_E\right) = \frac{1}{P} \cdot \sum_{p=1}^{P} I\left(\mathbf{W}_E\right)^{(p)}, \tag{20}$$

where P represents the number of gain segments. Furthermore, $I(\mathbf{W}_B)^{(p)}$ and $I(\mathbf{W}_E)^{(p)}$ correspond to the channel capacities of

the legitimate and eavesdropping links, when the channel gain falls within the p-th interval.

Furthermore, for a specific channel gain interval, following the transmitter's MIMO, modulation and bit polarization, the symmetric capacity expression becomes:

$$I\left(\mathbf{W}_B\right)^{(p)} = S \cdot \sum_{t=1}^{T_A} I\left(\mathbf{W}_t\right)^{(p)} = S \cdot \sum_{t=1}^{T_A} \sum_{j=1}^{m} I\left(\mathbf{W}_{t,j}\right)^{(p)}, \quad (21)$$

where S represents the total number of transmission time slots and m denotes the number of bits contained in each modulation symbol. Furthermore, $I(\mathbf{W}_{t,j})^{(p)}$ is the capacity of the MIMO-polarised bit sub-channel, which is given by:

$$I\left(\mathbf{W}_{t,j}\right)^{(p)} = \sum_{b_{t,j}} \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} \frac{1}{2^j} p_t\left(y_B \mid b_{t,j}\right) \cdot \log \frac{p_t\left(y_B \mid b_{t,j}\right)}{p_t\left(y_B \mid 1\right) p_t\left(y_B \mid 0\right)} du dv, \quad (22)$$

where y_B denotes the received signal, and $u = \Re\left(\mathrm{y}_B\right), v = \Im\left(\mathrm{y}_B\right)$. Furthermore, under the Gaussian-distributed input condition, the expression for $p_t\left(y_B \mid b_{t,j}\right)$ is:

$$p_t\left(y \mid b_{t,j}\right) = \frac{1}{2^{m-j}} \sum_{x_t} \frac{1}{\pi\sigma_B^2} \cdot \exp\left(\frac{-\|y_B - x_t\|^2}{\sigma_B^2}\right), \quad (23)$$

where x_t denotes the t-th antenna's transmitted signal in the legitimate link.

Simultaneously, the eavesdropper is unaware of the transmitter's specific MIMO-polarization design process, implying that it will encounter $T_A!$ signal detection patterns. Thus, the eavesdropper has a maximum probability of inferring the correct pattern given by $1/T_A!$, Hence the channel capacity of the eavesdropping link becomes:

$$I\left(\mathbf{W}_E\right)^{(p)} = \frac{S}{T_A!} \cdot \sum_{t=1}^{T_A} I\left(\mathbf{W}_t\right)^{(p)}. \quad (24)$$

Consequently, under the Gaussian-distributed input condition, the system's secrecy rate can be reformulated as:

$$I_{PLS} = \max\left\{0, I\left(\mathbf{W}_B\right) - \frac{1}{T_A!} \cdot I\left(\mathbf{W}_B\right)\right\}, \quad (25)$$

where $I\left(\mathbf{W}_B\right)$ is provided by Equation (19).

B. Finite-Alphabet Input

Taking into account a more practical scenario, the secrecy rate is formulated under finite symbol input conditions, representing the maximum positive difference between the achievable rates of the legitimate and eavesdropping links. To consolidate the expressions, we assume that the transmitter's transmit power is $\hat{\sigma}_B^2$, resulting in the secrecy rate expression:

$$R_{\mathrm{PLS}} = \max\left(0, R_B - R_E\right), \quad (26)$$

where R_B denotes the legitimate link's maximum achievable rate, while R_E represents the eavesdropper's maximum achievable rate.

As the transmit power increases, an upper bound on the legitimate link's achievable rate can be formulated as:

$$\lim_{\hat{\sigma}_{\mathrm{B}}^2 \to +\infty} R_{\mathrm{B}} = T_A \cdot \log_2 M. \quad (27)$$

Based on equation (27), for simplicity, we disregard the time index and express the legitimate link's achievable rate [41] under a given channel as:

$$R_B = T_A \cdot \log_2 M - \frac{1}{T_A \cdot M} \sum_{t=1}^{T_A} \sum_{k=1}^{M} E \left\{ \log_2 \left(1 + \sum_{\substack{t=1 \\ t \neq t'}}^{T_A} \exp\left(-\rho\left[\left(\mathbf{v}_{\mathrm{t,t'}} + \mathbf{z}_B\right)^{\dagger}\left(\mathbf{v}_{\mathrm{t,t'}} + \mathbf{z}_B\right) - \mathbf{z}_B^{\dagger}\mathbf{z}_B\right]\right) \right) \right\}, \quad (28)$$

where $\mathbf{v}_{t,t'} = \mathbf{H}_t x_k - \mathbf{H}_{t'} x_k$, $\mathbf{H}_t$ represents the first column through the t-th column of the original MIMO matrix $\mathbf{H}$ and $\rho = \hat{\sigma}_B^2/\sigma_B^2$ denotes the SNR.

Similarly, for the eavesdropper, there is only a $T_A!$ probability of inferring the correct MIMO detection sequence pattern. Hence, the eavesdropping link's achievable rate under this condition is expressed as:

$$R_E = \frac{1}{T_A!} \cdot R_B. \quad (29)$$

Thus, under the finite-alphabet input condition, the system's secrecy rate can be reformulated as:

$$R_{PLS} = \max\left\{0, R_B - \frac{1}{T_A!} \cdot R_B\right\} \quad (30)$$

As demonstrated by the aforementioned equation, as the number of transmit antenna and the power increase, the system's secrecy rate approaches the legitimate link's achievable rate. The eavesdropper's achievable rate is substantially reduced, resulting in a relatively high secrecy rate for the system.

V. Simulation result

In this section, we initially confirm that the proposed scheme exhibits a substantial performance enhancement compared to the conventional MIMO system. Then, we compare the performance of authorized users and eavesdroppers both in terms of their BER and BLER, thereby establishing the scheme's security enhancement. Subsequently, we present numerical results for the secrecy rate of the proposed method, considering both Gaussian distributed and discrete symbol input, which substantiates the efficiency of this approach. The simulation parameters are shown in Table III.

A. BER and BLER performance

As depicted in Fig. 7, MIMO-polarization transmission, modulation-polarization and bit-level polarization scheme, yields substantial performance improvements compared to conventional MIMO transmission. Explicitly, when we set the

TABLE III: Simulation parameters

Parameters	**Values**
Number of transmitter antennas T_A	2,4,8
Number of receiver antennas for legitimate N_B	1,2,4,8
Number of receiver antennas for eavesdropper N_E	1,2,4,8
Length of polar code N	512,1024
Length of information bits K	256,512
Number of channel segments P	1,4,8,16,32
MQAM modulation order M	2,4,16
Number of elements in the lists L	16
Number of CRC bits	24
Channel model	Rayleigh

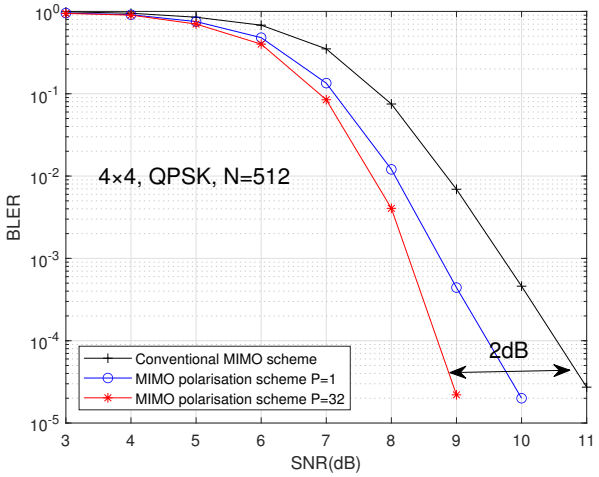
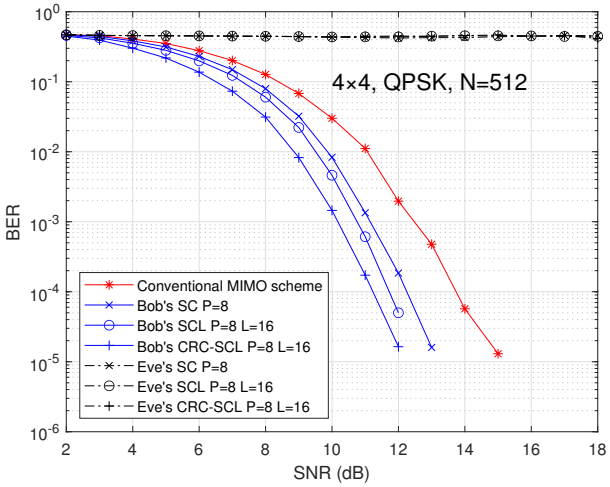
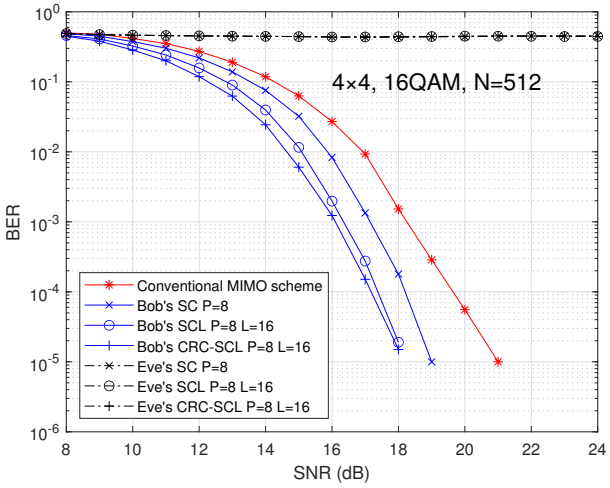


Fig. 7: BLER performance based on MIMO-polarization system versus conventional MIMO system.



(a) BER performance under $M = 4$.



(b) BER performance under $M = 16$.

Fig. 8: BER performance at Bob and Eve, where $N = 512$, $P = 8$ and $T_A = N_B = N_E = 4$. (a) QPSK, (b) 16QAM.

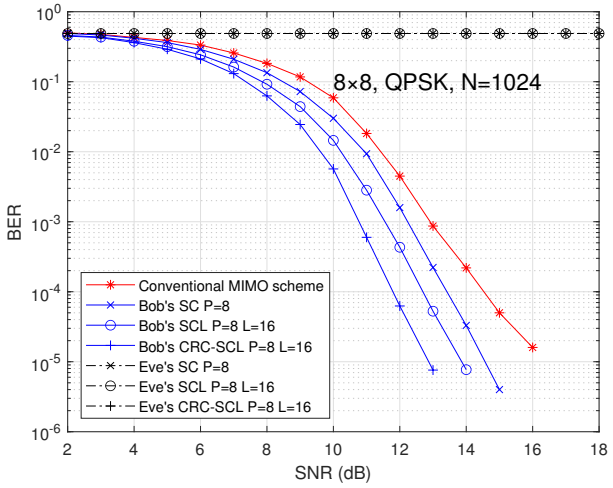
number of instantaneous channel gain intervals to $P = 32$, our scheme provides an improvement of about 2dB over a conventional MIMO scheme at BLER $\approx 2 \cdot 10^{-5}$. This enhancement is attributed to the increased polarization effect attained by our multi-domain polarization system, leading to improved bit subchannel reliability and more secure confidential information transmission for a given code length.

Fig. 8(a) characterizes the BER of both the legitimate party and of the eavesdropper, given a code length of $N = 512$. The number of instantaneous channel gain intervals was set to $P = 8$, and 4 transmit and receive antennas were used. Fig. 8(a) employs QPSK modulation, illustrating that as the SNR increases, Bob's BER is reduced rapidly, while Eve's BER remains approximately 0.5. When the high-performance decoding algorithms are employed 40, the legitimate party's BER improves, further, but the eavesdropper fails to glean any useful information. Comparable results are observed also for 16QAM, as shown in Fig. 8(b), which validates the benefits of the proposed scheme. Furthermore, it can be observed in Fig. 8 that the performance of the legitimate link is improved compared to the conventional MIMO scheme.

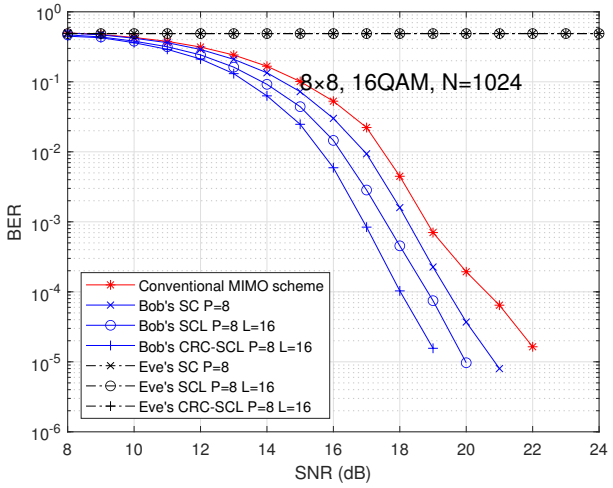
Let us how explore the impact of increasing the number of antennas and the code length, while enhancing the code length is known to improve the error correction performance of polar codes. Fig. 9 demonstrates the decoding performance when the code length is $N = 1024$, the number of instantaneous channel gain intervals is $P = 8$, and the number of transmit and receive antennas is 8. The trend observed aligns with that of Fig. 8. Regardless of whether high-order or low-order modulation is employed, the eavesdropper's bit error rate remains approximately 0.5, showing no improvement.Upon increasing the SNR, this is a testimony to the reliability of our PLS scheme based on MIMO-polarization.

Fig. 10 examines the influence of the number of channel gain intervals on the BLER of both the legitimate and eavesdropping links. As the number of intervals increases, the legitimate link's BLER performance improves, while the eavesdropper's performance degrades. Exploiting the segmented channel gain enhances the key randomness, making it more challenging for the eavesdropper to infer any useful information.

In order to characterize the achievable security perfor-



(a) BER performance under $M = 4$.



(b) BER performance under $M = 16$.

Fig. 9: BER performance at Bob and Eve, where $N = 1024, P = 8$ and $T_A = N_B = N_E = 8$. (a) QPSK, (b) 16QAM.

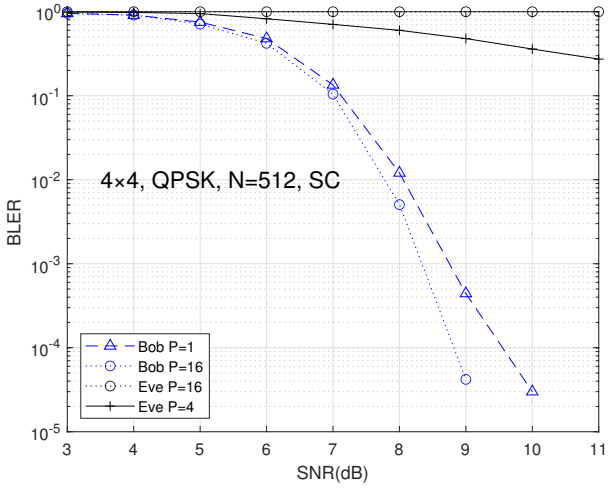


Fig. 10: BLER performance of Bob and Eve for different P values

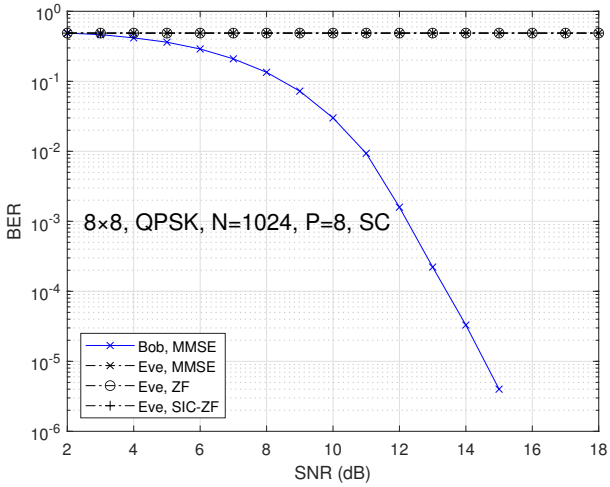


Fig. 11: BER performance at Bob and Eve, where Eve used different detection algorithms and $N = 1024, P = 8$ and $T_A = N_B = N_E = 8$.

mance of this scheme, we added simulation results, where the eavesdropper uses different detection algorithms. As shown in Fig.11, the eavesdropper still fails to decode a complete frame when using the zero forcing (ZF) detection algorithm and the serial interference cancellation (SIC-ZF) detection algorithm.

By observing Figs. 7, 8, 9, 10, 11, it becomes evident that the PLS scheme based on MIMO-polarization attains significant performance improvement, compared to conventional MIMO transmission.

B. Secrecy-rate results

In this subsection, we characterize the secrecy rate of the proposed scheme, with I_B denoting the channel capacity of the legitimate link, and I_P representing the system's secrecy rate.

1) Gaussian distributed input: Under the Gaussian distribution input condition, as depicted in Fig. 12, the secrecy rate of the proposed scheme approaches the channel capacity of the legitimate link, as the number of transmit antennas increases. Notably, when $T_A = 8$, the two values essentially coincide, demonstrating that the eavesdropper's decoding performance is significantly degraded under these conditions, ensuring the system's confidentiality. Additionally, the influence of the number of receive antennas and of the modulation scheme is also investigated. As illustrated in Fig. 13, the system's secrecy rate using BPSK is lower than that of QPSK, which is consistent with our theoretical expectations. Under both modulation schemes, the system's secrecy rate is very close to the legitimate link's channel capacity, confirming the system's practicality. Upon scrutinising Fig. 12 and Fig. 13, it becomes apparent that increasing the number of receive antennas, given the same number of transmit antennas and modulation scheme, has a certain impact on the system's rate due to the prior influence of data flow and interference from other antennas, which aligns with the theory.

Overall, under the Gaussian distributed input condition,

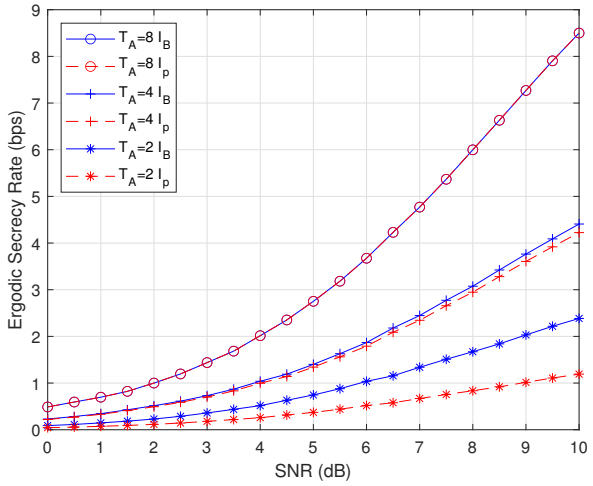


Fig. 12: The ergodic secrecy rate for Gaussian-distributed input, where $N = 1024, P = 8$, $N_B = N_E = T_A$ and QPSK is used.

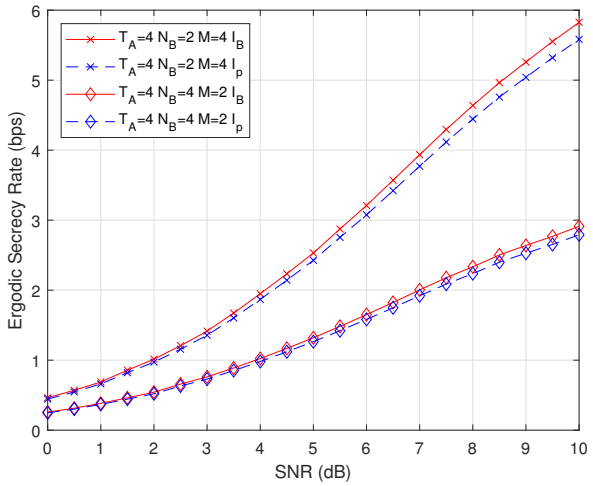


Fig. 13: The ergodic secrecy rate for Gaussian-distributed input, where $N = 1024, P = 8$ and N_B=N_E.

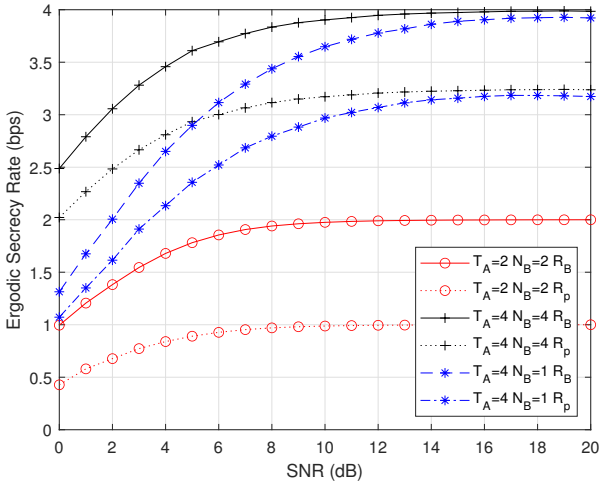


Fig. 14: The ergodic secrecy rate for Finite-Alphabet Input, where $N = 1024, P = 8$ and BPSK is used.

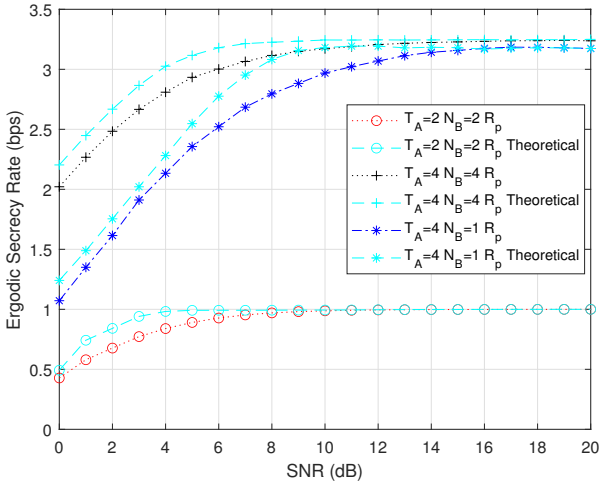


Fig. 15: The ergodic secrecy rate for Finite-Alphabet Input, also showing theoretical values related to BER, where $N = 1024, P = 8$ and BPSK is used.

the system's secrecy rate approaches the channel capacity of the legitimate link, as the number of transmit antennas increases, regardless of the choice of modulation scheme or the number of receive antennas. This observation is in line with the previously discussed BER performance and further validates the reliability of the proposed scheme.

2) Finite-Alphabet Input: In a more practical scenario, under the finite-alphabet input condition, this section presents the maximum achievable rate for both the legitimate link and the system. As depicted in Fig. 14, R_B represents the legitimate link's achievable rate, and R_p denotes the system's confidential achievable rate. Upon increasing the number of transmit antennas, the system's achievable rate gradually approaches that of the legitimate link, exhibiting a similar trend to that observed under the Gaussian distributed input condition, which substantiates the scheme's reliability. Furthermore, for the same number of transmit antennas, reducing the number of receive antennas has some impact on the system rate, but as the SNR increases, both upper limits become identical. This consistency with the theory does not affect the difference between the secrecy rate and the legitimate link's achievable rate.

Additionally, to verify that our multi-domain polarization-based design can enhance the system's overall polarization effect, the BER performance and secrecy rate are jointly analyzed. Under the same conditions, the legitimate link and eavesdropper's BER values are substituted into the binary symmetric channel (BSC) to obtain the secrecy rate as the theoretical value in the current situation. This is because polar codes have been shown to achieve the theoretical channel capacity of BSC. Upon comparing this theoretical value to the system's secrecy rate, wo can see in Fig. 15, that the difference between the two secrecy rates is minimal, and they converging as the SNR increases. This result demonstrates that

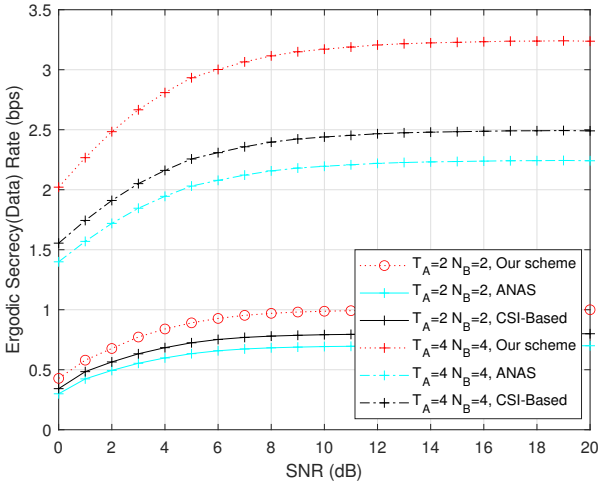


Fig. 16: The ergodic secrecy rate for Finite-Alphabet Input, also showing comparisons with existing schemes , where $N = 1024, P = 8$ and BPSK is used.

the proposed PLS scheme based on our multi-domain polarization design approaches the theoretical value under Rayleigh channel conditions, further corroborating the advantages of this approach.

To further validate the potential of the proposed scheme, We added a comparison to the above two schemes [8, 15], as shown in Fig. 16, observe that the ergodic secrecy rate of our proposed scheme is higher than that of the above two schemes. Compared to the AN and CSI based schemes, our scheme improves the secrecy rate of the system despite its reduced a overhead, which verifies the effectiveness of the proposed scheme.

VI. Conclusions

A novel physical layer security framework was conceived by leveraging both MIMO, modulation, and bit polarization. The proposed framework improves the legitimate link's performance, while significantly degrading the eavesdropper's reception to the point, where correctly decoding a complete data frame becomes nearly impossible. Furthermore, the channel's instantaneous gain is partitioned into segments to increase the key's randomness, hence again, improving the legitimate link's performance and degrading the eavesdropper's reception capability. The scheme's reliability is validated through simulations. Moreover, the system's secrecy rate is examined, and the numerical results demonstrate the scheme's confidentiality. It is worth mentioning that the receiver uses a simple cascaded design, and we will consider proposing more complex receiver architectures with better performance in our future work.

References

[1] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 20–27, 2015.

[2] M. Kamel, W. Hamouda, and A. Youssef, "Physical Layer Security in Ultra-Dense Networks," *IEEE Wireless Communications Letters*, vol. 6, no. 5, pp. 690–693, 2017.

[3] M. K. Islam and R. Liu, "Polar coding for fading channel," in *2013 IEEE Third International Conference on Information Science and Technology (ICIST)*, 2013, pp. 1096–1098.

[4] M. Gander and U. Maurer, "On the secret-key rate of binary random variables," in *Proceedings of 1994 IEEE International Symposium on Information Theory*, 1994, pp. 351–.

[5] A. Kalantari, M. Soltanalian, S. Maleki, S. Chatzinotas, and B. Ottersten, "Directional Modulation Via Symbol-Level Precoding: A Way to Enhance Security," *IEEE Journal of Selected Topics in Signal Processing*, vol. 10, no. 8, pp. 1478–1493, 2016.

[6] F. Shu, L. Xu, J. Wang, W. Zhu, and Z. Xiaobo, "Artificial-Noise-Aided Secure Multicast Precoding for Directional Modulation Systems," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 7, pp. 6658–6662, 2018.

[7] J. Hu, F. Shu, and J. Li, "Robust Synthesis Method for Secure Directional Modulation With Imperfect Direction Angle," *IEEE Communications Letters*, vol. 20, no. 6, pp. 1084–1087, 2016.

[8] X. Hu, C. Kai, S. Zhang, Z. Guo, and J. Gao, "To Establish a Secure Channel From a Full-Duplex Transmitter to a Half-Duplex Receiver: An Artificial-Noise-Aided Scheme," *IEEE Wireless Communications Letters*, vol. 8, no. 2, pp. 480–483, 2019.

[9] F. Shu, X. Wu, J. Li, R. Chen, and B. Vucetic, "Robust Synthesis Scheme for Secure Multi-Beam Directional Modulation in Broadcasting Systems," *IEEE Access*, vol. 4, pp. 6614–6623, 2016.

[10] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Design of an OFDM Physical Layer Encryption Scheme," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 3, pp. 2114–2127, 2017.

[11] X. Lu, Y. Shi, W. Li, J. Lei, and Z. Pan, "A Joint Physical Layer Encryption and PAPR Reduction Scheme Based on Polar Codes and Chaotic Sequences in OFDM System," *IEEE Access*, vol. 7, pp. 73 036–73 045, 2019.

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

[13] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: a tutorial," *IEEE Wireless Communications*, vol. 18, no. 2, pp. 66–74, 2011.

[14] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[15] F. Rottenberg, T.-H. Nguyen, J.-M. Dricot, F. Horlin, and J. Louveaux, "CSI-Based Versus RSS-Based Secret-Key Generation Under Correlated Eavesdropping," *IEEE Transactions on Communications*, vol. 69, no. 3, pp. 1868–1881, 2021.

[16] S. Wang, K. Huang, X. Xu, Z. Zhong, and Y. Zhou, "CSI-Based Physical Layer Authentication via Deep Learning," *IEEE Wireless Communications Letters*, vol. 11, no. 8, pp. 1748–1752, 2022.

[17] T. T. Tran and H. Y. Kong, "CSI-Secured Orthogonal Jamming Method for Wireless Physical Layer Security," *IEEE Communications Letters*, vol. 18, no. 5, pp. 841–844, 2014.

[18] H. Sharma, N. Kumar, R. K. Tekchandani, and N. Mohammad, "Deep Learning enabled Channel Secrecy Codes for Physical Layer Security of UAVs in 5G and beyond Networks," in *ICC 2022 - IEEE International Conference on Communications*, 2022, pp. 1–6.

[19] E. Hof, I. Sason, and S. Shamai, "Polar coding for reliable communications over parallel channels," in *2010 IEEE Information Theory Workshop*, 2010, pp. 1–5.

[20] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, 1993.

[21] U. Maurer and S. Wolf, "Unconditionally secure key agreement and the intrinsic conditional information," *IEEE Transactions on Information Theory*, vol. 45, no. 2, pp. 499–514, 1999.

[22] L. Li, Y. Xing, X. Yao, and Y. Luo, "McEliece Coding Method based on LDPC Code with Application to Physical Layer Security," in *2021 7th International Conference on Computer and Communications (ICCC)*, 2021, pp. 2042–2045.

[23] G. Yang and M. Zhuang, "Achieving the secrecy capacity on strong security using LT code with polar code pre-coding," in *2016 10th IEEE International Conference on Anti-counterfeiting, Security, and Identification (ASID)*, 2016, pp. 53–57.

[24] X. Bao, M.-M. Zhao, M. Lei, M. Zhao, and C. Wang, "Optimized Power Allocation for Secure Transmission Using Polar Code and Artificial Noise," in *2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*, 2019, pp. 1–5.

[25] S. Chen, S. Sun, Y. Wang, G. Xiao, and R. Tamrakar, "A comprehensive survey of TDD-based mobile communication systems from TD-SCDMA 3G to TD-LTE(A) 4G and 5G directions," *China Communications*, vol. 12, no. 2, pp. 40–60, 2015.

[26] Y. Ke, J. Liu, M.-Q. Zhang, T.-T. Su, and X.-Y. Yang, "Steganography Security: Principle and Practice," *IEEE Access*, vol. 6, pp. 73 009–73 022, 2018.

[27] A. Neri, D. Blasi, L. Gizzi, and P. Campisi, "Joint security and channel coding for OFDM communications," in *2008 16th European Signal Processing Conference*, 2008, pp. 1–5.

[28] A. Motamedi, M. Najafi, and N. Erami, "Parallel secure turbo code for security enhancement in physical layer," in *2015 Signal Processing and Intelligent Systems Conference (SPIS)*, 2015, pp. 179–184.

[29] E. Arikan, "Channel Polarization: A Method for Constructing Capacity-Achieving Codes for Symmetric Binary-Input Memoryless Channels," *IEEE Transactions on Information Theory*, vol. 55, no. 7, pp. 3051–3073, 2009.

[30] R. Hooshmand and M. R. Aref, "Efficient Polar Code-Based Physical Layer Encryption Scheme," *IEEE Wireless Communications Letters*, vol. 6, no. 6, pp. 710–713, 2017.

[31] Y. Yang and W. Li, "Security-Oriented Polar Coding Based on Channel-Gain-Mapped Frozen Bits," *IEEE Transactions on Wireless Communications*, vol. 21, no. 8, pp. 6584–6596, 2022.

[32] E. Arikan, "Systematic polar coding," *IEEE Communications Letters*, vol. 15, no. 8, pp. 860–862, 2011.

[33] W. Hao, L. Yin, and Q. Huang, "Secrecy Transmission Scheme Based on 2-D Polar Coding Over Block Fading Wiretap Channels," *IEEE Communications Letters*, vol. 22, no. 5, pp. 882–885, 2018.

[34] Z. B. K. Egilmez, L. Xiang, R. G. Maunder, and L. Hanzo, "The development, operation and performance of the 5G polar codes," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 96–122, 2019.

[35] J. Dai, K. Niu, and J. Lin, "Polar-Coded MIMO Systems," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 7, pp. 6170–6184, 2018.

[36] T. Mehmood, M. P. Yankov, S. Iqbal, and S. Forchhammer, "Flexible Multilevel Coding With Concatenated Polar-Staircase Codes for M-QAM," *IEEE Transactions on Communications*, vol. 69, no. 2, pp. 728–739, 2021.

[37] M. Seidl, A. Schenk, C. Stierstorfer, and J. B. Huber, "Polar-Coded Modulation," *IEEE Transactions on Communications*, vol. 61, no. 10, pp. 4108–4119, 2013.

[38] S. Park, "Low-Complexity LMMSE-Based Iterative Soft Interference Cancellation for MIMO Systems," *IEEE Transactions on Signal Processing*, vol. 70, pp. 1890–1899, 2022.

[39] L. Xiang, Y. Liu, R. G. Maunder, L.-L. Yang, and L. Hanzo, "Soft-Output Successive Cancellation Stack Polar Decoder," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 6, pp. 6238–6243, 2021.

[40] L. Xiang, Z. B. Kaykac Egilmez, R. G. Maunder, and L. Hanzo, "CRC-Aided Logarithmic Stack Decoding of Polar Codes for Ultra Reliable Low Latency Communication in 3GPP New Radio," *IEEE Access*, vol. 7, pp. 28 559–28 573, 2019.

[41] Y. Liu, Y. Yang, L.-L. Yang, and L. Hanzo, "Physical layer security of spatially modulated sparse-code multiple access in aeronautical *ad-hoc* networking," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 3, pp. 2436–2447, 2021.