Permutation Index DCSK Modulation Technique for Secure Multi-User High-Data-Rate Communication Systems

Marijan Herceg, *Member, IEEE*, Georges Kaddoum, *Member, IEEE*, Denis Vranješ, *Member, IEEE*
and Ebrahim Soujeri, *Senior Member, IEEE*

Abstract—A new non-coherent scheme called Permutation Index Differential Chaos Shift Keying (PI-DCSK) modulation is proposed in this paper. This original design aims to enhance data security, energy and spectral efficiencies, compared to its rivals. In the proposed PI-DCSK scheme, each data frame is divided into two time slots in which the reference chaotic signal is sent in the first time slot and a permuted replica of the reference signal multiplied by the modulating bit is sent in the second time slot. In particular, the bit stream is divided at the transmitter into blocks of $n + 1$ bits, where n mapped bits are used to select one of the predefined reference sequence permutations, while a single modulated bit is spread by the permuted reference signal just mentioned. At the receiver side, the reference signal is recovered first, then all permuted versions of it are correlated with the data-bearing signal. The index of the correlator output with maximum magnitude will estimate the mapped bits, while the output content of the corresponding correlator is compared to a zero threshold to recover the modulated bit. Moreover, a new multiple access (MA) method based on the proposed scheme is described and analysed. Analytical expressions for the error performance in single-user and multi-user environments are derived for additive white Gaussian noise (AWGN) and multipath Rayleigh fading channels, respectively. Furthermore, the performance of the proposed PI-DCSK system is analysed and compared with other non-coherent chaotic modulation schemes and is found to be promising.

Index Terms—Chaos-based communication systems, permutation index differential chaos shift keying (PI-DCSK), bit error rate (BER), non-coherent detection, multiple access (MA).

I. Introduction

CHAOTIC signals have gained increasing popularity for usage in spread spectrum communication systems in the last two decades. The main reason is that such signals can be easily generated and have properties like wideband spectrum, impulse-like auto-correlation and low cross-correlation values [1]. These properties are very important for better multiple access performance, higher resistance to jamming or interference and more immunity against multipath effects. Besides, its non-periodic nature reinforces the transmission security when, this latter, is used in a coherent fashion.

During previous researches numerous coherent and non-coherent chaos-based communication schemes have been proposed. The main drawback of coherent systems like chaos-shift-keying (CSK) [2] is the synchronization of chaotic signals at the receiver, which is a challenging task in noisy channels.

Enjoying excellent correlation properties of chaotic signals, non-coherent modulation schemes based on transmitted reference (TR) [3] method have been increasingly studied by the scientific community. The first non-coherent modulation based chaotic scheme is the differential chaos shift keying (DCSK) [4] and its constant power frequency-modulated DCSK version (FM-DCSK) [5]. In DCSK, every bit duration is split into two time slots. In the first slot, a reference chaotic sequence is sent, while in the second slot, a data-modulated time-delayed reference chaotic sequence is sent. At the receiver, the reference sequence is correlated with the data modulated sequence in order to recover the transmitted bit. The main advantages of such an approach are avoidance of chaotic sequence recovery, inexistence of a channel state estimator at the receiver, resistance to multi-path interferences and simple implementation. However, the main drawbacks of such an approach are low data rate, high energy consumption as well as the usage of wideband RF delay lines, which are not easy to implement in CMOS technology [6]. It should also be mentioned that the RF delay line is an issue only in analogue implementations, while in digital implementations, such as FPGA or system-on-chip (SoC), is no longer an issue.

Recently, some DCSK improvements on energy efficiency and data rate have been addressed in many works. In this vein, high-efficiency DCSK (HE-DCSK) is proposed in [7]. In HE-DCSK, bandwidth efficiency is doubled and chaotic signal re-transmission is reduced, which adds to the transmitted signal data security in comparison with DCSK. However, it needs four delay lines and is thus not suitable for fast fading channels. In order to reduce the number of needed delay lines in HE-DCSK, reference-modulated DCSK (RM-DCSK) has been proposed in [8]. In RM-DCSK, the reference chaotic signal also serves as a data bearer, which enhances bandwidth efficiency. To reduce the noise variance at the receiver, a noise-reduction DCSK (NR-DCSK) is proposed in [9]. In NR-

Marijan Herceg and Denis Vranješ are with the Department of Communications, Faculty of Electrical Engineering, Computer Science and Information Technology, Osijek, Croatia.　　(e-mails: mherceg@ferit.hr, denis.vranjes@ferit.hr)

Georges Kaddoum and Ebrahim Soujeri are with the University of Québec, École de technologie supérieure (ÉTS), LaCIME Laboratory, Montreal, Canada.　　(e-mails: georges.kaddoum@etsmtl.ca, esoujeri@ieee.org)

DCSK, multiple replicas of the reference chaotic signal are sent and averaged at the receiver in order to reduce the noise interference prior to correlation with the data bearing chaotic sequence. Short-reference DCSK (SR-DCSK) is proposed in [10] with the target of reducing delay lines. In SR-DCSK, a reference chaotic signal is shortened to less than a half of the bit duration and multiple replicas of the reference signal are used to spread the data. Such an approach improves energy efficiency and boosts data rate without adding hardware complexity. To improve spectral efficiency, quadrature chaos-shift keying (QCSK) is proposed in [11]. In QCSK, the reference chaotic signal is sent in the first slot, while a linear combination of the Hilbert transform of the reference signal and a delayed version of the reference signal are used to map two bits in the second slot. The non-coherent chaos-based permuted sequence technique is introduced in [12], in which permutations of the reference signal are used for mapping additional bits per transmitted symbol. Furthermore, to mitigate the effect of multipath fading and to achieve a full-scale diversity gain without the need to channel state information, space-time block codes (STBC) are used in combination with DCSK in [13].

To avoid the usage of wideband RF delay lines and double the data rate, the authors in [14] have proposed an improved DCSK (I-DCSK) in which a time-reversal operation on the reference sequence is used to separate the data and reference sequences, and the resultant symbol is transmitted in one time slot rather than two. Furthermore, the binary code-shifted DCSK (CS-DCSK) in which reference and data chaotic sequences are separated by Walsh codes instead of time delay multiplexing, is presented in [6]. Two multi-level versions of CS-DCSK, called generalized CS-DCSK (GCS-DCSK) and its improved version multi-level CS-DCSK (MCS-DCSK) are presented in [15] and [16], respectively. In high-data rate CS-DCSK (HCS-DCSK) [17], different chaotic sequences are used instead of Walsh codes in order to separate the reference and data sequences. However, such approaches need chaotic sequence synchronization at the receiver side. The implementation of DCSK-based communication systems in ultra-wideband (UWB) applications and cooperative communications (CC) is analysed in [18] and [19], respectively.

Multi-level, multi-carrier DCSK (MC-DCSK) in which the reference chaotic signal is sent over a predefined subcarrier frequency, while multiple modulated data streams are sent over the remaining orthogonal subcarriers was introduced in [20]. Despite the improvements achieved by such an approach with respect to energy efficiency and data rate, it demands large bandwidth.

Recently, the combination of index modulation (IM) and MC-DCSK, named carrier index DCSK (CI-DCSK) is proposed in [21]. In CI-DCSK, energy and spectral efficiency are enhanced by mapping a part of the bits in the subcarrier indices, i.e. to determine the subcarriers that will be active, while the remaining bits are conveyed by DCSK through these active carriers. To allow multiple-access and reduce bandwidth demands of MC-DCSK, a multi-user orthogonal-frequency-division-multiplexing DCSK (MU-OFDM-DCSK) is proposed in [22]. In MU-OFDM-DCSK, the spreading operation is performed in the time domain over multiple orthogonal frequencies. Each user is dedicated a set of predefined frequencies from multiple available frequencies, to transmit reference chaotic signals, while the remaining frequencies are shared with the other users to transmit multiple bits. In [20] and [21], the reference and data chaotic sequences are orthogonal over a chip time (the time duration of one chaotic sample), which requires the carrier time period to be less than the chip period. To reduce the demand on carrier frequencies, the frequency-translated DCSK (FT-DCSK) is proposed in [23]. In FT-DCSK, the orthogonality between reference and data chaotic sequences is sustained over a symbol duration, using an orthogonal sinusoid carrier. FT-DCSK has a lower demand on carrier frequencies compared to the methods proposed in [20] and [21], but is very sensitive to multipath time delays.

Recently, a novel $M-$ary modulation scheme called orthogonal multi-level DCSK (OM-DCSK) is proposed [24]. In this configuration, each data-bearing signal is chosen from a set of orthogonal chaotic sequences constructed from a reference signal. In order to increase the number of signals contained in the orthogonal signal set, chaotic sequences and their Hilbert transforms along with Walsh codes are used. The new scheme achieves a higher data rate, has an augmented energy efficiency and scores a better bit error rate (BER) performance.

Inspired by the works of [12], [14] and [24], we propose in this paper a multi-level permutation index DCSK (PI-DCSK) architecture. In the PI-DCSK scheme proposed here, the input bit stream is divided into blocks of $n+1$ bits transmitted at a time, where n bits are mapped in distinct permuted reference sequences and a single bit is physically transmitted.

Here, the n mapped bits are used to select one of the predefined reference sequence permutations while a single bit called the *modulated bit* is spread by the selected permuted sequence. This approach engages $n+1$ bits into each transmission instant. The remaining procedure in PI-DCSK has a similar structure to the conventional DCSK, where each data frame is separated into two time slots. In the first slot, the reference chaotic signal is sent and in the second slot, the modulated bit is transmitted after being spread by the selected permuted sequence.

At the receiver side, the reference signal is first recovered, then all possible permuted versions of it are correlated with the data bearing signal in order to find a maximum winner. The index of the winner correlator will estimate the mapped bits, while its content is used to provide an estimation of the modulated bit, after being compared to a zero threshold.

In the proposed design, the utilisation of 2^n quasi-orthogonal signals achieves a modulation order of $M = 2^{n+1}$. This fact enhances data rate and energy efficiency while it keeps hardware complexity relatively low. Furthermore, by eradicating the similarity between reference and data bearing signals through using different permutations, the transmitted data security of the proposed scheme is enhanced.

Furthermore, by exploiting the possible permutation set size, a new multiple access (MA) method is proposed. Namely, for a given chaotic sequence length β, there is $\beta! - 1$ possible permutations. In order to allow the MA in PI-DCSK, a distinct set of 2^n permutations is used for each user.

Compared to OM-DCSK, PI-DCSK avoids the usage of repeated chaotic generators (RCG), Hilbert transforms or Walsh codes at the transmitter and receiver sides. The fact that we put aside Walsh codes in PI-DCSK equips the proposed system with all properties of non-coherent modulation.

To complete the proposed scheme, analytical bit error rate (BER) expressions over Rayleigh multipath fading and additive white Gaussian noise (AWGN) channels, in both single-user and multi-user environments are derived and validated versus simulation results. This is to show the extent and level of accuracy of our analytical expressions. Finally, the performance of PI-DCSK is analysed and compared with rival modulation techniques to show its superiority.

The remainder of this paper is organized as follows: In Section II, the PI-DCSK system model is briefly described. System analysis is provided in section III. Performance analysis of PI-DCSK system over AWGN and multipath Rayleigh channels is provided in section IV. Simulation results and discussions are presented in Section V while conclusions are given in section VI.

II. PI-DCSK SYSTEM MODEL

In this section, the transmitter and receiver architectures of the proposed system will be described in detail.

A. The transmitter

A block diagram of the proposed PI-DCSK system is presented in Fig. 1, where the transmitter is shown in (a), the permutation process in (b) and the receiver in (c). At the transmitter, the chaotic generator generates a chaotic sequence of β samples that is used as a reference signal and is placed in the first time slot. This reference signal is simultaneously loaded into a permutation block in order to generate different permuted replicas of the original reference signal in the second time slot. Permutations are chosen in a way such that it provides quasi-orthogonality between the generated permuted reference signal replicas. An efficient method for generating a suitable set of permuted sequences with the aforementioned properties from the reference sequence is proposed in [25]. Moreover, it is demonstrated that for a large spreading factor, permuted replicas of a chaotic signal are quasi-orthogonal to each other [25] such that

$$\mathbf{x}P_j(\mathbf{x})^T \approx 0, \tag{1}$$

$$P_i(\mathbf{x})P_j(\mathbf{x})^T \approx 0, \text{ for } i \neq j, \tag{2}$$

where $\mathbf{x}$ is a vector that contains β number of chaotic samples, $P_j(\cdot)$ represents the jth permutation operator and $(\cdot)^T$ denotes transposition. Therefore, to carry n mapped bits, each transmitter will generate 2^n distinct permutations. By using a method described in [25], the $\beta-1$ permutations can be easily generated.

In particular, the input signed bit stream is divided at the PI-DCSK modulator into blocks of $n+1$ bits. The ith block of bits of the kth user can be written as $\left[a_{i,1}^{(k)}, a_{i,2}^{(k)}, \cdots, a_{i,n+1}^{(k)}\right] = \left[\mathbf{s}_i^{(k)}, a_{i,n+1}^{(k)}\right]$, where $\mathbf{s}_i^{(k)} = \left[a_{i,1}^{(k)}, a_{i,2}^{(k)}, \cdots, a_{i,n}^{(k)}\right]$ is the vector of n mapped bits.

The mapped bits $\mathbf{s}_i^{(k)}$ select one of the 2^n predefined permutations $\mathbf{P}^{(k)} = \{P_1^{(k)}, P_2^{(k)}, \cdots, P_{2^n}^{(k)}\}$. Each element in $\mathbf{s}_i^{(k)}$ is a code vector generated by introducing a permutation of the original reference sequence, as indicated earlier, while the modulated bit denoted by $a_{i,n+1}^{(k)}$ is spread by the selected permuted sequence. Note that by using this mapping approach, the overall PI-DCSK modulation order becomes equal to $M = 2^{n+1}$ by using only $M/2 = 2^n$ quasi-orthogonal signals.

Furthermore, asynchronous data transmission of different users is assumed in this paper. In addition, in the PI-DCSK system, each user uses a distinct set of $M/2$ permutations, such that $\mathbf{P}^{(k)} \cap \mathbf{P}^{(u)} = \emptyset$, for $k \neq u$. In general, the overall number of possible permutations that can be performed on a reference chaotic sequence of length β is equal to $\beta! - 1$. This allows us to assign different sets of chaotic codes to a large number of users without having scarcity of spreading sequences. In this vein, by permuting a reference signal of length β, the number of users N_u in the PI-DCSK system is theoretically very large and is bound to

$$N_u \leq (\beta! - 1)/(M/2). \tag{3}$$

By using the proposed MA method, even for moderate spreading factors β, the possible number of users grows to large values because the number of users in PI-DCSK system is proportional to the different permutation that can be performed on the reference signal. This fact constitutes a great advantage for multi-user scenarios. For example, for $\beta = 50$, the total number of users turns to be $N_u \approx 1.52 \times 10^{64}$ users, for $M = 4$. However, it should be stated that not all permutations, out from set of $\beta! - 1$ permutations, have a low cross-correlation property and therefore, the system performance may degrade if permutations are not properly chosen.

The discrete baseband vector representation of the kth user, i^{th} PI-DCSK symbol that contains $n+1$ bits, can be expressed as

$$\mathbf{e}_i^{(k)} = \left[\mathbf{x}_{i,0}^{(k)} \ a_{i,n+1}^{(k)} P_j^{(k)}\left(\mathbf{x}_{i,\beta}^{(k)}\right)\right], \tag{4}$$

where $\mathbf{x}_{i,v}^{(k)}$ is the kth user, i^{th} vector of β chaotic samples, with time delay v, defined as

$$\mathbf{x}_{i,v}^{(k)} = \left[x_{i,1-v}^{(k)}, x_{i,2-v}^{(k)}, \cdots, x_{i,\beta-v}^{(k)}\right]. \tag{5}$$

In (4), $\mathbf{x}_{i,0}^{(k)}$ is the reference signal vector of β delay-free chaotic samples while $\mathbf{x}_{i,\beta}^{(k)}$ is a replica of the reference signal delayed by β samples. Moreover, $P_j^{(k)}(\cdot)$ represents the permutation operation of the kth user, for the ith block of mapped bits $\mathbf{s}_i^{(k)}$, while $j \in \{1, 2, \cdots, M/2\}$ represents the index of the selected permutation. The PI-DCSK frame architecture is shown in Fig 1 (b). Furthermore, it is clear from (4) that the symbol duration in PI-DCSK is equal to $T_s = 2\beta T_c$, where T_c is the chip duration and 2β is the spreading factor.

B. The receiver

In this paper, a commonly used channel model in wireless communications [20], [26] is considered. In this model, the kth

user, l^{th} path channel coefficient and time delay are denoted as $\lambda_{l,k}$ and $\tau_{l,k}$, respectively. It should be noted that in this work, all L_k channel coefficients are considered to be flat and quasi-static over the transmission period of one frame and that they are i.i.d. random variables that follow a Rayleigh distribution. The Rayleigh probability density function (PDF) of the channel coefficients is given by

$$f_\lambda(z) = \frac{z}{\sigma^2} \; e^{-z^2/2\sigma^2}, \tag{6}$$

where $\sigma > 0$ is the distribution scale parameter representing the root mean square value of the received signal before envelope detection.

Therefore, when the transmitted signal passes through the Rayleigh fading channel, the received signal of the kth user, i^{th} symbol can be stated as

$$\mathbf{r}_i^{(k)} = \sum_{l=1}^{L_k} \lambda_{l,k} \left[\mathbf{x}_{i,\tau_{l,k}}^{(k)} \quad a_{i,n+1}^{(k)} P_j^{(k)} \left(\mathbf{x}_{i,\beta+\tau_{l,k}}^{(k)} \right) \right]$$
$$+ \sum_{\substack{u=1 \\ u \neq k}}^{N_u} \sum_{l=1}^{L_u} \lambda_{l,u} \left[\mathbf{R}_{i,\tau_{l,u}}^{(u)} \quad \mathbf{D}_{i,\tau_{l,u}}^{(u)} \right] + \left[\mathbf{n}_{i,0,k}^R \quad \mathbf{n}_{i,0,k}^D \right], \tag{7}$$

where the vector $\mathbf{R}_{i,\tau_{l,u}}^{(u)}$ is the uth user transmitted signal of β chaotic samples, which describes the kth user reference time slot, while the vector $\mathbf{D}_{i,\tau_{l,u}}^{(u)}$ is the uth user signal of β chaotic samples, which characterizes the kth user data time slot, respectively. More, L_u is the number of paths for the uth user, while the vectors $\mathbf{n}_{i,0,k}^R$ and $\mathbf{n}_{i,0,k}^D$ are the noise components of the kth user, i^{th} data frame that occur during the reference and data time slots, respectively. These noise vectors are respectively defined as

$$\mathbf{n}_{i,0,k}^R = [n_{i,1,k}, \cdots, n_{i,\beta,k}], \tag{8}$$

$$\mathbf{n}_{i,0,k}^D = [n_{i,\beta+1,k}, \cdots, n_{i,2\beta,k}], \tag{9}$$

where $n_{i,v,k}$ is an AWGN sample with zero mean and a variance $N_0/2$.

At the receiver, as shown in Fig. 1 c), the reference signal is loaded in the permutation block during the first time slot i.e., $[iT_s, (2i+1)T_s/2]$. Then, $M/2$ permutations $\{P_1^{(k)}, P_2^{(k)}, \cdots, P_{M/2}^{(k)}\}$ of the reference sequence are performed and stored. Furthermore, all permuted reference sequences are simultaneously correlated with the data bearing sequence during the second time slot of duration $[(2i+1)T_s/2, (i+1)T_s,]$, forming $M/2$ decision variables.

The corresponding decision variable at the output of the kth

user, i^{th} time slot, m^{th} correlator may be stated as

$$D_{i,m}^{(k)} = P_m^{(k)} \left(\sum_{l=1}^{L_k} \lambda_{l,k} \mathbf{x}_{i,\beta+\tau_{l,k}}^{(k)} \right.$$
$$\left. + \sum_{\substack{u=1 \\ u \neq k}}^{N_u} \sum_{l=1}^{L_u} \lambda_{l,u} \mathbf{R}_{i,\beta+\tau_{l,u}}^{(u)} \quad + \mathbf{n}_{i,\beta,k}^R \right)$$
$$\times \left(\sum_{l=1}^{L_k} \lambda_{l,k} a_{i,n+1}^{(k)} P_j^{(k)} (\mathbf{x}_{i,\beta+\tau_{l,k}}^{(k)}) \right.$$
$$\left. + \sum_{\substack{u=1 \\ u \neq k}}^{N_u} \sum_{l=1}^{L_u} \lambda_{l,u} \mathbf{D}_{i,\tau_{l,u}}^{(u)} \quad + \mathbf{n}_{i,0,k}^D \right)^T, 1 \leq m \leq M/2. \tag{10}$$

In order to determinate the matching permutation index, in the detector and decision logic circuit, the magnitude of $M/2$ correlator outputs, are compared in order to find the largest value

$$\hat{j} = \arg\max_m \left\{ \left| D_{i,m}^{(k)} \right| \right\}, m \in \{1, 2, \cdots, M/2\}. \tag{11}$$

By estimating the index of the largest correlator's output $\hat{j}$, the receiver knows which permutation is used and uses the index of that permutation to provide an estimation of the n mapped bits. The physically modulated bit can then be recovered by computing the sign of the selected correlator

$$\hat{a}_{i,n+1}^{(k)} = \text{sgn}(D_{i,\hat{j}}^{(k)}). \tag{12}$$

In our analysis, we assume that the largest delay, over all possible user and path combinations $\tau_{\max}$ is much shorter than duration of the reference signal, i.e.

$$0 < \tau_{\max} << \beta T_c. \tag{13}$$

where $\tau_{\max} = \max(\tau_{l,k})$ for all k, l. With this assumption in hand, the inter symbol interference (ISI) may be neglected.

III. SYSTEM ANALYSIS

In this section, a PI-DCSK system analysis regarding energy efficiency and data security is provided. Furthermore, hardware complexity comparison with OM-DCSK is performed as the two systems share similar hardware functionalities and properties.

A. Energy efficiency

Besides its simplicity and high spectral efficiency, another major advantage of the PI-DCSK is its energy efficiency. In [20], the authors have introduced the data-energy-to-bit-energy ratio (DBR) as

$$\text{DBR} = \frac{E_{\text{data}}}{E_b}, \tag{14}$$

where E_{data} is the energy of data bearing signal, while E_b is the required total energy to carry each bit. In the proposed PI-DCSK scheme, the symbol energy E_s is expressed as

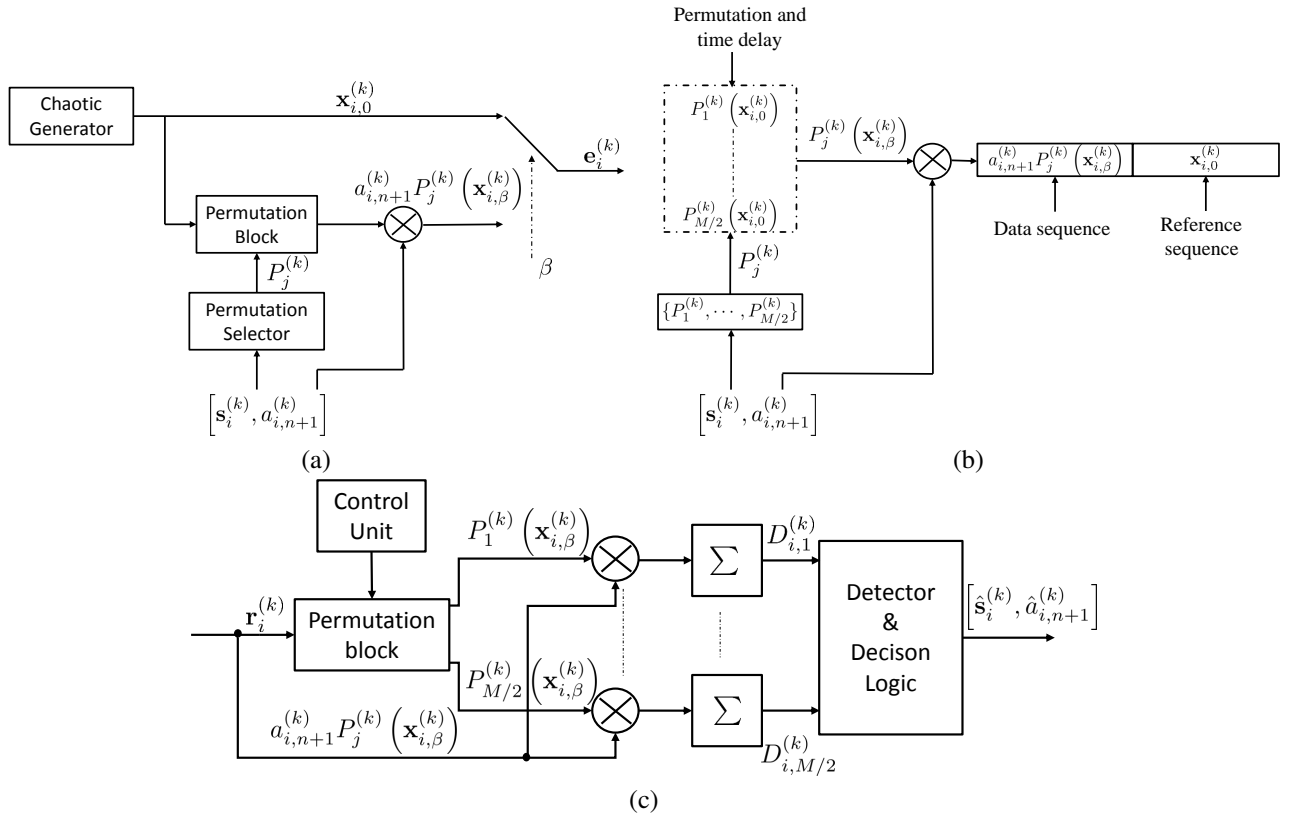$$E_s = E_{\text{data}} + E_{\text{ref}}, \tag{15}$$

Fig. 1: A block diagram of the general structure of PI-DCSK communication system. a) transmitter, b) frame architecture c) receiver.

where E_{ref} is the energy of the reference sequence. Since the data sequence is a permuted version of the reference sequence, the reference and data energies are equal

$$E_{\text{data}} = E_{\text{ref}} = T_c \sum_{k=1}^{\beta} x_{i,k}^2. \tag{16}$$

Thus, the PI-DCSK symbol energy is equal to

$$E_s = 2T_c \sum_{k=1}^{\beta} x_{i,k}^2. \tag{17}$$

In fact, E_s used to transmit $\log_2(M) = n+1$ bits while E_{ref} is used to carry the reference signal. Therefore, in comparison to the conventional transmit reference scheme, the energy required to transmit one bit would be

$$E_b = \frac{E_s}{\log_2(M)} = \frac{2T_c}{\log_2(M)} \sum_{k=1}^{\beta} x_{i,k}^2. \tag{18}$$

Subsequently, by using (15), (16), (17) and (18), the DBR in (14) can be rewritten as

$$\text{DBR} = \frac{E_{\text{data}}}{E_b} = \frac{\log_2(M)}{2}. \tag{19}$$

Table I shows the DBR of different chaotic modulations. As clearly indicated in (14), the DBR can be simply denoted as the ratio of the number of bits per symbol to the number of chaotic sequences needed to transmit that symbol. For example, in DCSK, two chaotic sequences (reference and data)

Modulation	DBR
DCSK, CS-DCSK	$1/2$
HE-DCSK, RM-DCSK, QCSK, FT-DCSK	$2/3$
MCS-DCSK	$(M-2)/M$
MC-DCSK	$(M-1)/M$
OM-DCSK, PI-DCSK	$\log_2(M)/2$

TABLE I: DBR comparison of different chaotic modulation techniques

are used to transmit one bit. It can be seen from Table I that the DBR values of both MC-DCSK and MCS-DCSK converge to unity for higher values of M, while this ratio is logarithmic in the order of M for PI-DCSK and OM-DCSK, which is advantageous. Further, in the proposed PI-DCSK system, the DBR is higher than unity because n bits are mapped in the permutation, while only one bit is physically transmitted. Therefore, with only one reference and one data sequence, $n+1$ bits are transmitted. Note that a higher DBR value is an indication of a higher non-coherent modulation energy efficiency.

B. Data security

In conventional DCSK systems, bit rate can be easily detected by analyzing the frequency spectrum of the squared DCSK signal. This arises from the fact that when squaring the DCSK signal, both reference and data bearing signals become equal. This equality is translated into the frequency spectrum as zero values at *odd* multiple frequencies of the bit

rate [25]. However, when a data-bearing signal is constructed from different reference signal permutations, the similarity between reference and data bearing signals is eradicated and, therefore, the frequency spectrum of the squared PI-DCSK signal remains white. Furthermore, in order to properly demodulate the PI-DCSK signal, $M/2$ permutations should be known at the receiver. Therefore, if some unintended receiver, i.e., a fraudulent one, tries to demodulate the signal, it should first find these $M/2$ permutations from the set of $\beta! - 1$ possible permutations. In fact, according to the security standard described in [27], a system is deemed secure if a fraudulent receiver needs to perform at least 128! trials in order to find the appropriate permutation set. Therefore, the proposed PI-DCSK can be considered secure for $\beta > 128$.

C. Hardware complexity comparison with OM-DCSK

In this section, the PI-DCSK hardware complexity is compared with the OM-DCSK for the same modulation order M, as they share similar modulation properties. Table II and Table III show the elements that are needed to construct PI-DCSK and OM-DCSK transmitters and receivers, respectively.

In summary, PI-DCSK avoids the usage of Walsh code

Transmitter	PI-DCSK	OM-DCSK
Adders	0	1
Multipliers	1	$2M$
Spectral efficiency	$\log_2(M)/(2\beta)$	$\log_2(M)/\beta$
Additional blocks	Permutation block, single switch	Walsh code generator, Hilbert transformer, RCG

TABLE II: Transmitter complexity comparison of PI-DCSK and OM-DCSK.

Receiver	PI-DCSK	OM-DCSK
Adders	$M/2$	M
Multipliers	$M/2$	$2M$
Additional blocks	Permutation block	Walsh code generator, Hilbert transformer

TABLE III: Receiver complexity comparison of PI-DCSK and OM-DCSK.

generators, Hilbert transforms and repeated chaotic generators (RCG). As observed in Table II, the spectral efficiency of the OM-DCSK seems to be double that of the PI-DCSK. This is because OM-DCSK is using I/Q channels for transmitting reference and data bearing signals. However, PI-DCSK may also transmit using I/Q channels and achieve a similar spectral efficiency. Furthermore, PI-DCSK transmitters do not need any adders at all and need a single multiplier while OM-DCSK transmitters need an adder and $2M$ multipliers. Therefore, the complexity of the proposed PI-DCSK is reduced to a great extent in comparison with OM-DCSK.

Similarly, the PI-DCSK receiver needs only half the number of adders and quarter the number of multipliers needed by OM-DCSK, regardless of M. By the same token, permutation blocks remain the only additional instrument needed on both sides of the PI-DCSK system.

IV. PERFORMANCE ANALYSIS

In this section, the performance of PI-DCSK is evaluated, and analytical BER expressions are derived for AWGN and multipath Rayleigh fading channels. We employ the Chebyshev polynomial function in this work because of its simplicity and excellent statistical properties [28]. For simplicity, the chip time T_c is set to unity. This polynomial is known to proceed as

$$x_{i,k} = 1 - 2x_{i,k-1}^2. \tag{20}$$

In addtion, the chaotic samples are normalized such that their mean values are all zero and their variance is unity i.e., $E(x_{i,k}) = 0$, and $E(x_{i,k}^2) = 1$, where $E(\cdot)$ is the expectation operator. To obtain the system performance analysis, the Gaussian approximation (GA) method has been used. GA is accurate for large spreading factors but shows some inaccuracy for smaller spreading factors [29]. However, large spreading factors are the basic property of spread-spectrum communication systems, which makes GA suitable for analysis in chaos-based communication systems.

A. BER analysis of PI-DCSK

In every PI-DCSK transmission, $\log_2(M) = n + 1$ bits are sent, where n bits map into permutation indices and a single bit is modulated. Hence, the BER of the PI-DCSK system is composed of the BER of the mapped bits Pr_{map} and the BER of the modulated bit Pr_{mod}. Therefore, the total BER Pr_M would be expressed as [30]

$$Pr_M = \frac{n}{\log_2(M)}Pr_{\mathrm{map}} + \frac{1}{\log_2(M)}Pr_{\mathrm{mod}}. \tag{21}$$

The probability of BER for mapped bits Pr_{map} is dependent upon the number of mapped bits n and the probability of erroneous permutation index detection Pr_{ed}. Furthermore, if the permutation is erroneously detected, a wrong combination of mapped bits will be estimated. Each wrong combination may contain a different number of incorrect bits, compared to the correct combination. Thereupon, the probability of erroneous permutation detection can be converted into a corresponding mapped bits BER by using [31]

$$Pr_{\mathrm{map}} = \frac{2^{(n-1)}}{2^n - 1}Pr_{\mathrm{ed}}. \tag{22}$$

The correct estimation of the modulated bit depends on the correct permutation index detection and the correct despreading process. Accordingly, two different cases cause an error to occur. In the first case, the permutation index is correctly detected but an error occurs while despreading the modulated bit. Note that the despreading process in PI-DCSK is performed in the same fashion as in conventional DCSK. In the second case, the permutation index is erroneously estimated and the modulated bit is despread at the output of the wrong correlator. In this case, the probability of correct detection will be simply equal to $\frac{1}{2}$. Consequently, the total BER of modulated bits would be expressed as [30]

$$Pr_{\mathrm{mod}} = Pr_{\mathrm{DCSK}}(1 - Pr_{\mathrm{ed}}) + 0.5Pr_{\mathrm{ed}}, \tag{23}$$

where Pr_{DCSK} is the BER for DCSK. Using (21), (22) and (23), the detailed form of Pr_M is revealed as

$$Pr_M = \frac{Pr_{\text{DCSK}}}{\log_2(M)}\left(1 - Pr_{\text{ed}}\right) + \frac{2n2^{n-1} + (2^n - 1)}{2\log_2(M)(2^n - 1)}Pr_{\text{ed}}. \quad (24)$$

B. Erroneous permutation detection probability Pr_{ed}

In order to estimate the transmitted permutation index, the PI-DCSK detector and decision logic circuits select the maximum absolute value that is obtained at the output of one of the 2^n engaged correlators. For equiprobable transmitted permuted sequences, the error probability conditioned on the kth user transmitted permutation $P_j^{(k)}$ is given by

$$Pr_{\text{ed}} = Pr\left(\left|D_{i,j}^{(k)}\right| < \max\left(\left|D_{i,m}^{(k)}\right|\right)\Big|P_j^{(k)}\right),$$
$$\text{for} \quad 1 \leq \underset{m \neq j}{m} \leq 2^n, \quad (25)$$

where $D_{i,m}^{(k)}$ and $D_{i,j}^{(k)}$ are the decision variables at the mth and j^{th} correlator outputs, respectively. In agreement with (25), an erroneous permutation index estimation will occur if the maximum absolute value of the decision variable $\left|D_{i,m}^{(k)}\right|$ is larger than $\left|D_{i,j}^{(k)}\right|$.

As observed in (10), the ith data block decision variable of the kth user at the output of the mth correlator may follow two different patterns according two hypotheses. The first hypothesis is when the index of the correlator output M is equal to the transmitted permutation index j, i.e $j = m$, where $1 \leq m \leq 2^n$, while the second hypothesis is when the index of the correlator output does not match the index of transmitted permutation i.e., $m \neq j$. Subsequently, the decision variable defined in (10) can be rewritten as

$$D_{i,m}^{(k)} = \begin{cases} S_{i,j}^{(k)} + \text{MUI}_{i,j}^{(k)} + N_{i,j}^{(k)}, & \text{for} \quad m = j, \\ I_{i,m}^{(k)} + \text{MUI}_{i,m}^{(k)} + N_{i,m}^{(k)}, & \text{for} \quad m \neq j, \end{cases} \quad (26)$$

where $S_{i,j}^{(k)}$ represents the desired signal, $\text{MUI}_{i,j}^{(k)}$ and $\text{MUI}_{i,m}^{(k)}$ are the multi user interference (MUI) components, $N_{i,m}^{(k)}$ and $N_{i,j}^{(k)}$ are interference components generated by Gaussian noise and $I_{i,m}^{(k)}$ is the interference that models the cross-correlation of different permuted chaotic sequences. As such, the desired signal $S_{i,j}^{(k)}$ can be rewritten from (10) as

$$S_{i,j}^{(k)} = \left(\sum_{l=1}^{L_k} \lambda_{l,k} P_j^{(k)}\left(\mathbf{x}_{i,\beta+\tau_{l,k}}^{(k)}\right)\right)$$
$$\times \left(\sum_{l=1}^{L_k} \lambda_{l,k} a_{i,n+1}^{(k)} P_j^{(k)}(\mathbf{x}_{i,\beta+\tau_{l,k}}^{(k)})\right)^T$$
$$= \sum_{l=1}^{L_k} \lambda_{l,k}^2 a_{i,n+1}^{(k)} P_j^{(k)}(\mathbf{x}_{i,\beta+\tau_{l,k}}^{(k)}) P_j^{(k)}(\mathbf{x}_{i,\beta+\tau_{l,k}}^{(k)})^T$$
$$+ \sum_{l=1}^{L_k}\sum_{\substack{l'=1 \\ l' \neq l}}^{L_k} \lambda_{l,k}\lambda_{l',k} a_{i,n+1}^{(k)} P_j^{(k)}(\mathbf{x}_{i,\beta+\tau_{l',k}}^{(k)}) P_j^{(k)}(\mathbf{x}_{i,\beta+\tau_{l,k}}^{(k)})^T$$
$$\approx a_{i,n+1}^{(k)}\sum_{k=1}^{\beta}\sum_{l=1}^{L_k}\lambda_{l,k}^2\left(x_{i,k-\tau_{l,k}}^{(k)}\right)^2. \quad (27)$$

The last approximation in (27) occurs as a result of the low auto-correlation property of time-shifted chaotic sequences [17]

$$\mathbf{x}_{i,\tau_{l,k}}^{(k)}\left(\mathbf{x}_{i,\tau_{l',k}}^{(k)}\right)^T \approx 0, \qquad \text{for} \quad l \neq l'. \quad (28)$$

Therefore, the mean value of the ith data block at the jth correlator output, conditioned on a given $a_{i,n+1}^{(k)}$, is

$$E\left(D_{i,j}^{(k)}|a_{i,n+1}^{(k)}\right) \approx a_{i,n+1}^{(k)}\frac{\log_2(M)E_b}{2}\sum_{l=1}^{L_k}\lambda_{l,k}^2. \quad (29)$$

The approximation in (29) arises from the assumption that $\tau_{max} << \beta T_c$, which means that ISI is negligible.

From (10), $\text{MUI}_{i,j}^{(k)}$ can be restated as

$$\text{MUI}_{i,j}^{(k)} = \sum_{\substack{u=1 \\ u \neq k}}^{N_u}\sum_{l=1}^{L_u}\lambda_{l,u}P_j^{(k)}\left(\mathbf{R}_{i,\beta+\tau_{l,u}}^{(u)}\right)$$
$$\times \left(\sum_{l=1}^{L_k}\lambda_{l,k}a_{i,n+1}^{(k)}P_j^{(k)}(\mathbf{x}_{i,\beta+\tau_{l,k}}^{(k)}) + \sum_{\substack{u=1 \\ u \neq k}}^{N_u}\sum_{l=1}^{L_u}\lambda_{l,u}\mathbf{D}_{i,\tau_{l,u}}^{(u)}\right)^T$$
$$+ \sum_{l=1}^{L_k}\lambda_{l,k}P_j^{(k)}\left(\mathbf{x}_{i,\beta+\tau_{l,k}}^{(k)}\right)\left(\sum_{\substack{u=1 \\ u \neq k}}^{N_u}\sum_{l=1}^{L_u}\lambda_{l,u}\mathbf{D}_{i,\tau_{l,u}}^{(u)}\right)^T. \quad (30)$$

Due to the low cross-correlation between different permuted chaotic sequences, as described in (1) and (2), the multi-user interference $\text{MUI}_{i,j}^{(k)}$ can be modelled as a zero mean Gaussian variable with variance

$$\text{var}\left(\text{MUI}_{i,j}^{(k)}\right) =$$
$$\sum_{\substack{u=1 \\ u \neq k}}^{N_u}\sum_{l=1}^{L_u}\sum_{l'=1}^{L_k} E\left(\left[\lambda_{l,u}\lambda_{l',k}a_{i,n+1}^{(k)}P_j^{(k)}\left(\mathbf{R}_{i,\beta+\tau_{l,u}}^{(u)}\right)\right.\right.$$
$$\left.\left.\times\left(P_j^{(k)}(\mathbf{x}_{i,\beta+\tau_{l',k}}^{(k)})\right)^T\right]^2\right)$$
$$+ \sum_{\substack{u=1 \\ u \neq k}}^{N_u}\sum_{\substack{u'=1 \\ u' \neq k}}^{N_u}\sum_{l=1}^{L_u}\sum_{l'=1}^{L_u} E\left(\left[\lambda_{l,u}\lambda_{l',u'}P_j^{(k)}\left(\mathbf{R}_{i,\beta+\tau_{l,u}}^{(u)}\right)\right.\right.$$
$$\left.\left.\times\left(\mathbf{D}_{i,\tau_{l',u'}}^{(u')}\right)^T\right]^2\right)$$
$$+ \sum_{l=1}^{L_k}\sum_{\substack{u=1 \\ u \neq k}}^{N_u}\sum_{l'=1}^{L_u} E\left(\left[\lambda_{l,k}\lambda_{l',u}P_j^{(k)}\left(\mathbf{x}_{i,\beta+\tau_{l,k}}^{(k)}\right)\left(\mathbf{D}_{i,\tau_{l',u}}^{(u)}\right)^T\right]^2\right)$$
$$\approx (N_u - 1)\frac{\log_2^2(M)E_b^2}{2\beta}\sum_{l=1}^{L_k}\lambda_{l,k}^2 + (N_u - 1)^2\frac{\log_2^2(M)E_b^2}{4\beta}. \quad (31)$$

The last approximation in (31) emerges from two standard assumptions. The first assumption is that the expectation of the squared product of two different chaotic sequences is equal to [14], [32]

$$E\left(\left[\mathbf{x}_{i,v}^{(u)}P_j^{(k)}\left(\mathbf{x}_{i,v}^{(k)}\right)\right]^2\right) = E\left(\left[P_z^{(k)}\left(\mathbf{x}_{i,v}^{(u)}\right)P_j^{(k)}\left(\mathbf{x}_{i,v}^{(k)}\right)\right]^2\right)$$
$$= \frac{\log_2^2(M)E_b^2}{4\beta}, \qquad \text{for} \quad z \neq j \quad \text{and} \quad u \neq k. \quad (32)$$

The second assumption is that the overall mean energy of a channel with L_u paths is equal to

$$\sum_{l=1}^{L_u} E\left(\lambda_{l,u}^2\right) = 1. \tag{33}$$

Furthermore, the noise interference component of the ith data block at the jth correlator output can be written as

$$
\begin{aligned}
N_{i,j}^{(k)} &= \sum_{\substack{u=1 \\ u \neq k}}^{N_u} \sum_{l=1}^{L_u} \lambda_{l,u} P_j^{(k)} \left(\mathbf{R}_{i,\beta+\tau_{l,u}}^{(u)}\right) (\mathbf{n}_{i,0,k}^D)^T \\
&+ P_j^{(k)} \left(\mathbf{n}_{i,\beta,k}^R\right) \left(\sum_{\substack{u=1 \\ u \neq k}}^{N_u} \sum_{l=1}^{L_u} \lambda_{l,u} \mathbf{D}_{i,\tau_{l,u}}^{(u)}\right)^T \\
&+ \left(\sum_{l=1}^{L_k} \lambda_{l,k} P_j^{(k)} \left(\mathbf{x}_{i,\beta+\tau_{l,k}}^{(k)}\right)\right) (\mathbf{n}_{i,0,k}^D)^T \\
&+ P_j^{(k)}(\mathbf{n}_{i,\beta,k}^R) \left(\sum_{l=1}^{L_k} \lambda_{l,k} a_{i,n+1}^{(k)} P_{j^{(i)}}^{(k)} \left(\mathbf{x}_{i,\beta+\tau_{l,k}}^{(k)}\right)\right)^T \\
&+ P_j^{(k)}(\mathbf{n}_{i,\beta,k}^R)(\mathbf{n}_{i,0,k}^D)^T.
\end{aligned}
\tag{34}
$$

In (34), all terms are uncorrelated, while channel coefficients and noise samples are independent. Hence, the variance of $N_{i,j}^{(k)}$ can be easily written as

$$
\begin{aligned}
\text{var}(N_{i,j}^{(k)}) &= (N_u - 1)N_0 \frac{\log_2(M)E_b}{2} \\
&+ N_0 \frac{\log_2(M)E_b}{2} \sum_{l=1}^{L_k} \lambda_{l,k}^2 + \beta \frac{N_0^2}{4}.
\end{aligned}
\tag{35}
$$

Subsequently, the overall variance of the kth user, j^{th} correlator decision variable is equal to

$$
\begin{aligned}
\text{var}\left(D_{i,j}^{(k)}\right) &= \text{var}\left(\text{MUI}_{i,j}^{(k)}\right) + \text{var}\left(N_{i,j}^{(k)}\right) \\
&\approx (N_u - 1)\frac{\log_2^2(M)E_b^2}{2\beta} \sum_{l=1}^{L_k} \lambda_{l,k}^2 + (N_u - 1)^2 \frac{\log_2^2(M)E_b^2}{4\beta} \\
&+ (N_u - 1)N_0 \frac{\log_2(M)E_b}{2} \\
&+ N_0 \frac{\log_2(M)E_b}{2} \sum_{l=1}^{L_k} \lambda_{l,k}^2 + \beta \frac{N_0^2}{4}.
\end{aligned}
\tag{36}
$$

Furthermore, by using the properties mentioned in (1) and (2), the disturbance component $I_{i,m}^{(k)}$ in (26) is approximately equal to zero, because of the low cross-correlation between different permuted replicas

$$
\begin{aligned}
I_{i,m}^{(k)} &= \left(\sum_{l=1}^{L_k} \lambda_{l,k} P_m^{(k)}(\mathbf{x}_{i,\beta+\tau_{l,k}}^{(k)})\right) \\
&\times \left(\sum_{l=1}^{L_k} \lambda_{l,k} a_{i,n+1}^{(k)} P_j^{(k)}(\mathbf{x}_{i,\beta+\tau_{l,k}}^{(k)})\right)^T \approx 0.
\end{aligned}
\tag{37}
$$

Using the same techniques as in (31) and (34), it can be easily shown that the variances of $\text{MUI}_{i,m}^{(k)}$ and $N_{i,m}^{(k)}$ are equal to the variances of $\text{MUI}_{i,j}^{(k)}$ and $N_{i,j}^{(k)}$, respectively. Subsequently, the overall variance of the kth user, m^{th} correlator, where $m \neq j$, decision variable would be stated as

$$
\begin{aligned}
\text{var}\left(D_{i,m}^{(k)}\right) &= \text{var}\left(\text{MUI}_{i,m}^{(k)}\right) + \text{var}\left(N_{i,m}^{(k)}\right) \\
&\approx (N_u - 1)\frac{\log_2^2(M)E_b^2}{2\beta} \sum_{l=1}^{L_k} \lambda_{l,k}^2 + (N_u - 1)^2 \frac{\log_2^2(M)E_b^2}{4\beta} \\
&+ (N_u - 1)N_0 \frac{\log_2(M)E_b}{2} \\
&+ N_0 \frac{\log_2(M)E_b}{2} \sum_{l=1}^{L_k} \lambda_{l,k}^2 + \beta \frac{N_0^2}{4}.
\end{aligned}
\tag{38}
$$

It is important to note that due to the absolute value operator, the mean value of $\left|D_{i,j}^{(k)}\right|$ is independent of the modulated bit value and hence $a_{i,n+1}^{(k)}$ will be omitted in the derivations that shall follow. The absolute values of the $2^n - 1$ random variables $\left|D_{i,m}^{(k)}\right|$ follow folded normal distribution due to the fact that $D_{i,m}^{(k)}$ is a zero mean Gaussian random variable [33]. Moreover, they are independent and hence, order statistics theory can be applied to compute (25) as [30]

$$Pr_{\text{ed}} = 1 - \int_0^\infty \left(F_{\left|D_{i,m}^{(k)}\right|}(y)\right)^{2^n - 1} f_{\left|D_{i,j}^{(k)}\right|}(y)dy, \tag{39}$$

where $F_{\left|D_{i,m}^{(k)}\right|}(y)$ is the cumulative distribution function (CDF) of $\left|D_{i,m}^{(k)}\right|$ given as

$$F_{\left|D_{i,m}^{(k)}\right|}(y) = \text{erf}\left(\frac{y}{\sqrt{2\text{var}\left(D_{i,m}^{(k)}\right)}}\right), \tag{40}$$

where $\text{erf}(\cdot)$ is error function given as

$$\text{erf}(z) = \int_0^z \frac{2}{\sqrt{\pi}} e^{-x^2} dx. \tag{41}$$

More, $f_{\left|D_{i,j}^{(k)}\right|}(y)$ is the probability density function (PDF) of the folded normally distributed random variable $\left|D_{i,j}^{(k)}\right|$ which is given as

$$
\begin{aligned}
f_{\left|D_{i,j}^{(k)}\right|}(y) &= \frac{1}{\sqrt{2\pi\text{var}\left(D_{i,j}^{(k)}\right)}}\left[\exp\left(-\frac{\left(y-E\left(D_{i,j}^{(k)}\right)\right)^2}{2\text{var}\left(D_{i,j}^{(k)}\right)}\right)\right. \\
&\left.+ \exp\left(-\frac{\left(y+E\left(D_{i,j}^{(k)}\right)\right)^2}{2\text{var}\left(D_{i,j}^{(k)}\right))}\right)\right].
\end{aligned}
\tag{42}
$$

By substituting $\gamma_b = E_b/N_0 \sum_{l=1}^{L_k} \lambda_{l,k}^2$ in the expressions (28), (30) and (33), we may rewrite (37) as

$$
\begin{aligned}
Pr_{\text{ed}} &= 1 - \frac{1}{\sqrt{\pi W}} \int_0^\infty \left(\text{erf}\left(\frac{y}{\sqrt{W}}\right)\right)^{2^n - 1} \\
&\times \left[\exp\left(-\frac{\left(y - \frac{\log_2(M)}{2}\gamma_b\right)^2}{W}\right)\right. \\
&\left.+ \exp\left(-\frac{\left(y + \frac{\log_2(M)}{2}\gamma_b\right)^2}{W}\right)\right] dy,
\end{aligned}
\tag{43}
$$

where

$$W = (N_u - 1)\frac{\log_2^2(M)}{\beta}\left(\frac{E_b}{N_0}\gamma_b + \frac{(N_u - 1)}{2}\left(\frac{E_b}{N_0}\right)^2\right)$$
$$+ (N_u - 1)\log_2(M)\frac{E_b}{N_0} + \log_2(M)\gamma_b + \frac{\beta}{2}. \quad (44)$$

C. BER of modulated bit

In order to estimate the modulated bit, the despreading process is performed as in conventional DCSK, by comparing the decision variable $D_{i,j}^{(k)}$ to a zero threshold. Then, by using (29) and (36), the bit error rate probability Pr_{DCSK} would be scripted as

$$Pr_{\text{DCSK}} = \frac{1}{2}\text{erfc}\left(\frac{E\left(D_{i,j}^{(k)}\right)}{\sqrt{2\text{var}\left(D_{i,j}^{(k)}\right)}}\right), \quad (45)$$

where $\text{erfc}(x) = 1 - \text{erf}(x)$ is the complementary error function. After some straightforward operations, the instantaneous BER probability of DCSK system would be noted as

$$Pr_{\text{DCSK}} = \frac{1}{2}\text{erfc}\left(\frac{\log_2(M)\gamma_b}{2\sqrt{W}}\right), \quad (46)$$

where W is as mentioned in (45). The bit energy E_b can be assumed to be constant for higher spreading factors β. Therefore, for L_k independent identically distributed (i.i.d.) Rayleigh-fading channels, the PDF of instantaneous γ_b can be written as [31]

$$f(\gamma_b, \bar{\gamma}_c, L_k) = \frac{\gamma_b^{L_k-1}}{(L_k - 1)!\,\bar{\gamma}_c^{L_k}}\exp\left(-\frac{\gamma_b}{\bar{\gamma}_c}\right), \quad (47)$$

where $\bar{\gamma}_c$ is equal to

$$\bar{\gamma}_c = \frac{E_b}{N_0}E\left(\lambda_{l,k}^2\right) = \frac{E_b}{N_0}E\left(\lambda_{j,k}^2\right), l \neq j. \quad (48)$$

For dissimilar channels, however, the PDF of γ_b can be written as

$$f(\gamma_b) = \sum_{l=1}^{L_k}\frac{\rho_l}{\bar{\gamma}_l}\exp\left(-\frac{\gamma_b}{\bar{\gamma}_l}\right), \quad (49)$$

where

$$\rho_l = \prod_{\substack{j=1 \\ j\neq l}}^{L_k}\frac{\bar{\gamma}_l}{\bar{\gamma}_l - \bar{\gamma}_j}. \quad (50)$$

Notice that for $L_k = 1$ and $\lambda_{1,k} = 1$ the channel reduces to AWGN. Finally, the averaged BER of the PI-DCSK system over multipath Rayleigh fading channels is given as

$$\bar{P}r_{M\text{fad}} = \int_0^\infty Pr_M f(\gamma_b)d\gamma_b, \quad (51)$$

where the integral in (51) is evaluated numerically.

V. RESULTS AND DISCUSSIONS

In this section, the performance of the proposed PI-DCSK scheme is evaluated. In Monte-Carlo simulation, the Chebyshev polynomial function is used for the generation of chaotic samples. The performance analysis is carried out for AWGN and multipath Rayleigh fading channels. To analyse the performance in multipath Rayleigh fading channels, three different channel profiles are used. In the first channel model named CM1, a two-ray channel is used with an average power gain of $E\left(\lambda_1^2\right) = E\left(\lambda_2^2\right) = 1/2$. The second channel model named CM2 uses a three-ray channel with the following gains $E\left(\lambda_1^2\right) = 4/7, E\left(\lambda_2^2\right) = 2/7, E\left(\lambda_3^2\right) = 1/7$. Finally, the third channel model named CM3 uses a five-ray channel with equal gains in all five paths, i.e., $E\left(\lambda_i^2\right) = 1/5$, where $i = 1, \cdots, 5$. For all multipath channel profiles, the delay spreads are varying according to the uniform distribution between zero and a, where $a \ll \beta T_c$.

A. Performance evaluation

In order to verify our theoretical derivations, the results obtained in (51) are validated by Monte-Carlo simulation over AWGN, CM1, CM2 and CM3 channels. First, the averaged
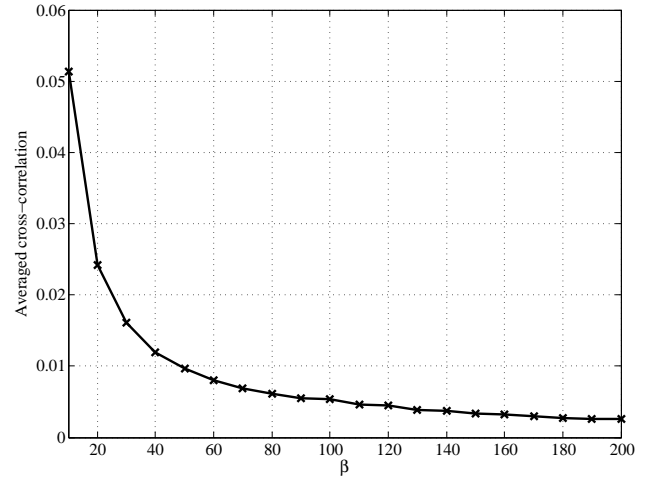

Fig. 2: Averaged cross-correlation of two differently permuted sequences for various β.

cross-correlations, defined as (2), of two differently permuted sequences chosen as in [25], are shown in Fig. 2, for different β. The cross-correlations are calculated and averaged for 1000 different permuted sequences. It can be seen that the cross correlation is low and exponentially decreases when the spreading factor increases.

In Figs. 3-4, the influence of different modulation orders M on the PI-DCSK BER performance over AWGN and the multipath Rayleigh fading channels CM1, CM2 and CM3 is shown. As observed in these figures, there is a perfect match between the BER results obtained by the analytical expressions of (24) and (51), versus Monte-Carlo simulation. Predictably, as M increases the PI-DCSK BER performance improves, which is due to the fact that for higher M, more bits are mapped within a symbol for the same transmitted energy and, hence, the required E_b/N_0 needed to achieve a
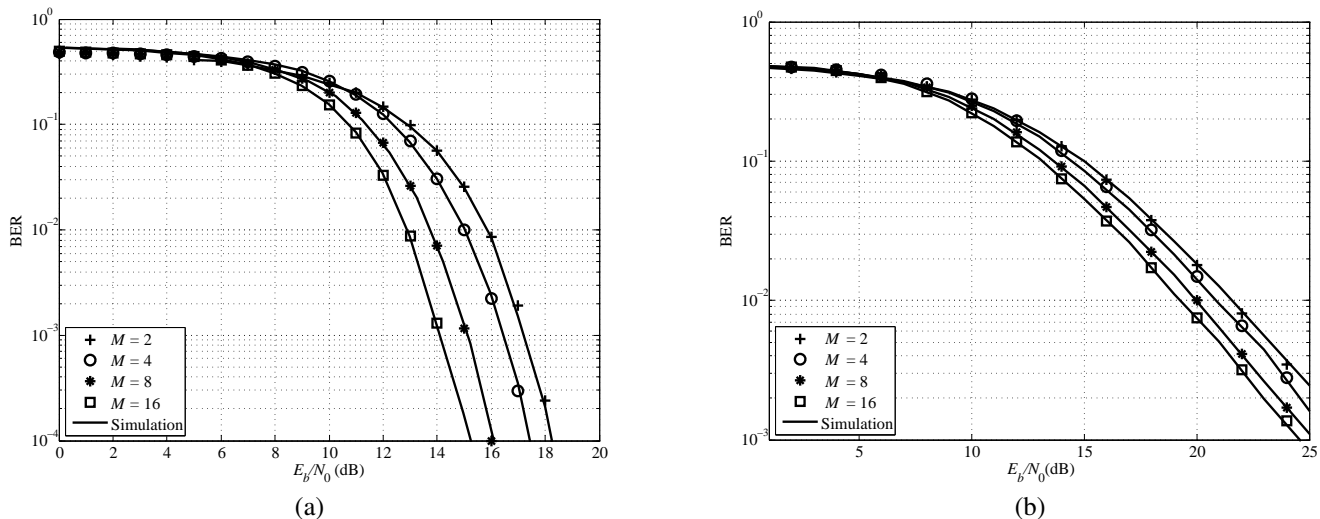
Fig. 3: The influence of different modulation orders M on PI-DCSK performance for β = 200 over (a) AWGN and (b) CM1 channels.

certain BER performance reduces. Furthermore, it should be noticed that the BER performance of PI-DCSK for $M = 2$ is equal to the conventional DCSK. For example, Fig. 3 (a) clearly indicates that in order to achieve a BER of 10^{-3}, the required E_b/N_0 level for PI-DCSK must be approximately 3 dB lower for $M = 16$ in comparison to $M = 2$. In other words, when M increases, the number of bits per PI-DCSK frame increases, while the transmitted energy remains constant. This explains the obtained performance behaviour and proves the high energy efficiency of the system. Furthermore, it is evident that there is a perfect match between theoretical and simulation results for all channel models, which validates our analytical approach. In Figs. 5-6 respectively, the influence of different spreading sequence length β on the PI-DCSK BER performance over AWGN and multipath Rayleigh fading channels CM1, CM2 and CM3 is shown. It is obvious that when β increases the PI-DCSK BER performance degrades. This is owing to the fact that for higher values of β, the noise×noise cross correlation terms in (36) and (38) become more significant, which causes the degradation of PI-DCSK BER performance. To show the validity limit of our assumption, we plotted the BER performance over CM3. Hence, the gap between analytical and simulation results over CM3, which occurs for $\beta = 50, 100$, is caused by the ISI interference that is neglected in the derivation of the analytical expressions. Therefore, to have an idea about the optimal spreading factor values, the BER curves of PI-DCSK versus spreading sequence length β for various modulation orders M, are plotted in Fig. 7. It is shown that for a given E_b/N_0 ratio, there exists an optimal spreading sequence length β within the range from 5 to 40, which optimizes the BER performance. If we let β_{opt} to indicate the optimal value of β, we observe that β_{opt} is dynamic and keeps an incremental trend as the modulation order M increases. For example, at $E_b/N_0 = 14$ dB, $\beta_{\text{opt}} < 10$ for $M = 2$, while this value is $\beta_{\text{opt}} \approx 50$ for $M = 16$. Furthermore, it can be seen that the BER performance deteriorates as the spreading factor β escalates, despite the increment of quasi-orthogonality between

differently permuted replicas of the reference sequence for larger β values. This is because the contribution of the noise-noise cross terms of (36) and (37) is more significant than the increment of quasi-orthogonality between the two permuted sequences, as the spreading sequence grows.

The effect of ISI on BER performance is shown in Fig. 8. The results are obtained for CM1 channel profile with $E_b/N_0 = 16$ dB and $\beta = 200$. It is clear that ISI can be neglected when the channel delay spread is much lower than the symbol duration, as expected. However, for larger delay spreads the influence of this interference increases significantly, which causes a mismatch between theoretical BER expressions that assume zero ISI and the simulated system performance.

B. Multiple access performance

To evaluate the effects of the number of users on PI-DCSK, the BER performance for three and six users are examined, over AWGN and fading channels.

In Fig. 9, PI-DCSK BER performance over CM2 is shown for the modulation orders $M = 2, 16$, a spreading factor of $\beta = 300$ and $N_u = 3$ users. As illustrated, the best performance is obtained when $M = 2$. It arises from the fact that when the number of users rises, the MUI variance expressions in (36) and (38) increase the overall noise level at each correlator output. Subsequently, as the decision logic will have to choose between $M/2$ correlator outputs, there will be a higher possibility that an error will occur in the estimation of the permutation index (mapped bits), which increases the BER and leads to performance deterioration.

In Figs. 10-12 respectively, the influence of the spreading sequence length on MUI interference in a multi-user scenario, over AWGN, CM2 and CM3 channels for $M = 4$, is shown. As highlighted, when the number of users increases from 3 to 6 the BER increases, i.e the performance degrades, for a fixed β value, i.e. $\beta = 100$. However, when β increases to 300, the MUI variance is additionally spread, which decreases the overall BER and enhances performance. To conclude, in
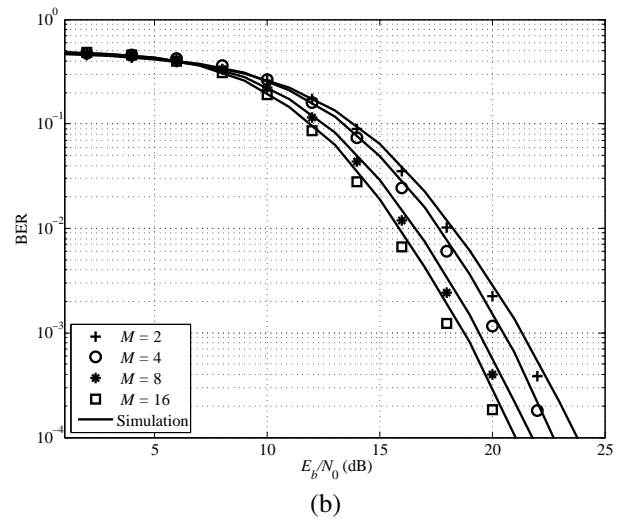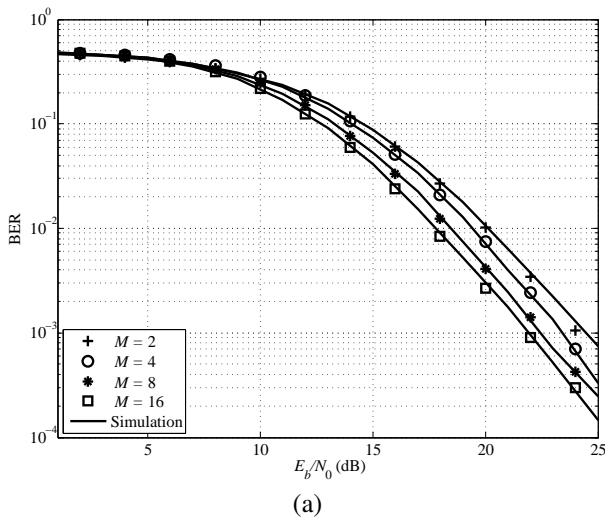
Fig. 4: The influence of different modulation orders M on PI-DCSK performance for $\beta = 200$ over (a) CM2 and (b) CM3 channels.
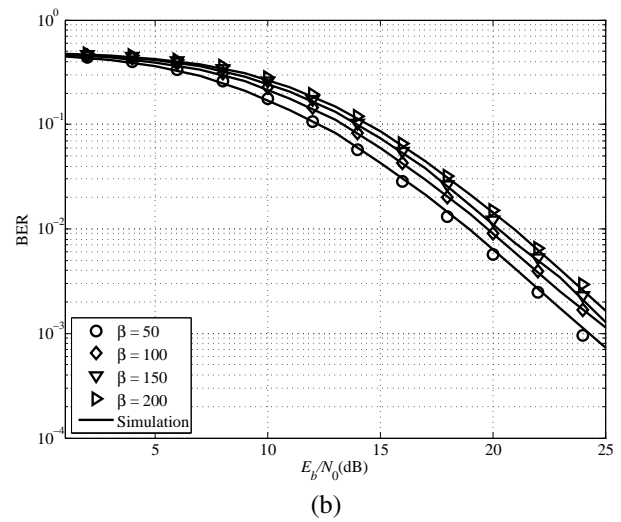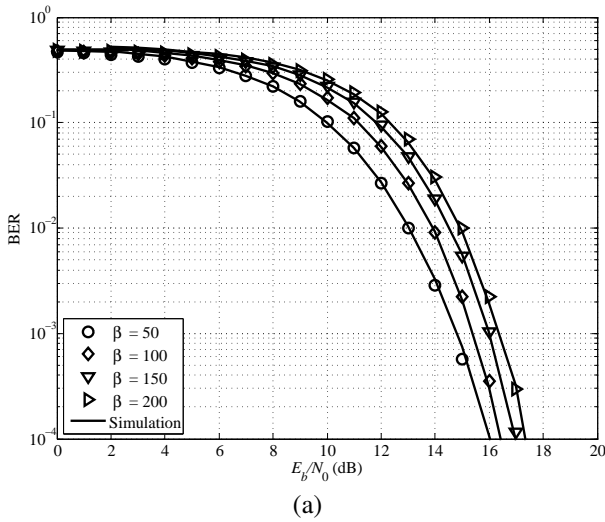

Fig. 5: The influence of β on PI-DCSK performance for $M = 4$ over (a) AWGN and (b) CM1 channels.
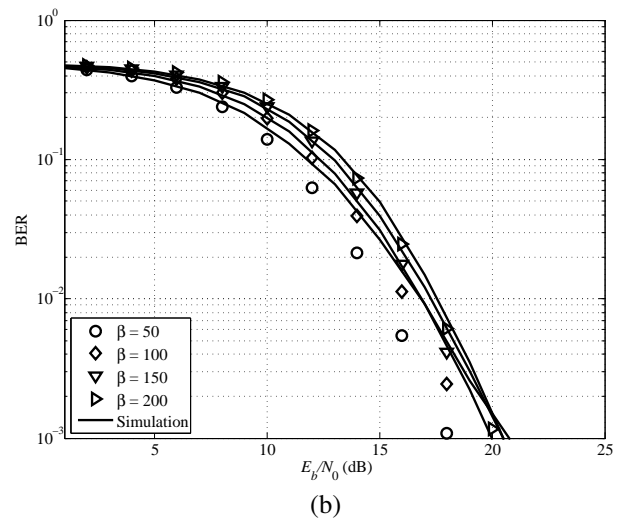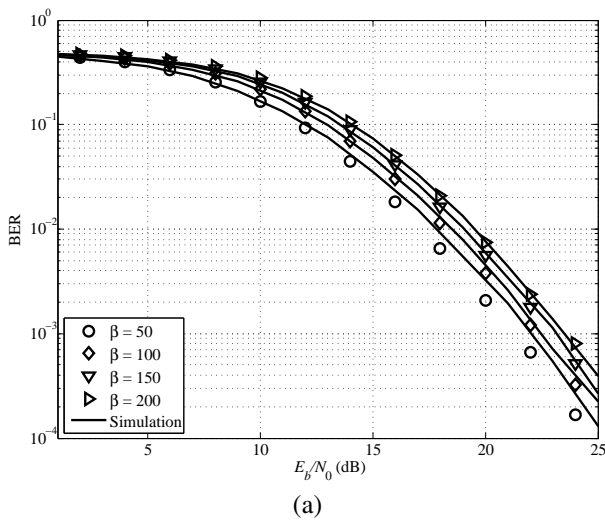

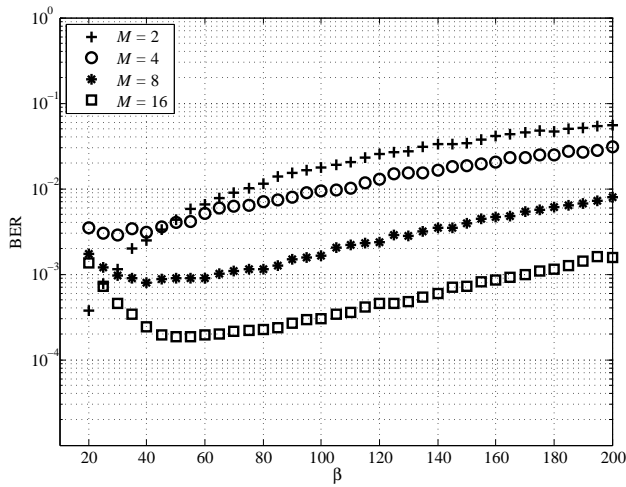Fig. 6: The influence of β on PI-DCSK performance for $M = 4$ over (a) CM2 and (b) CM3 channels.

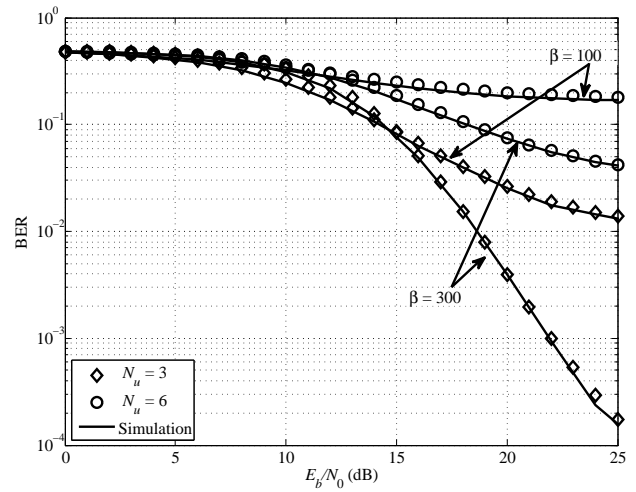Fig. 7: The BER performance of PI-DCSK at $E_b/N_0 = 14$ dB for various β and M.

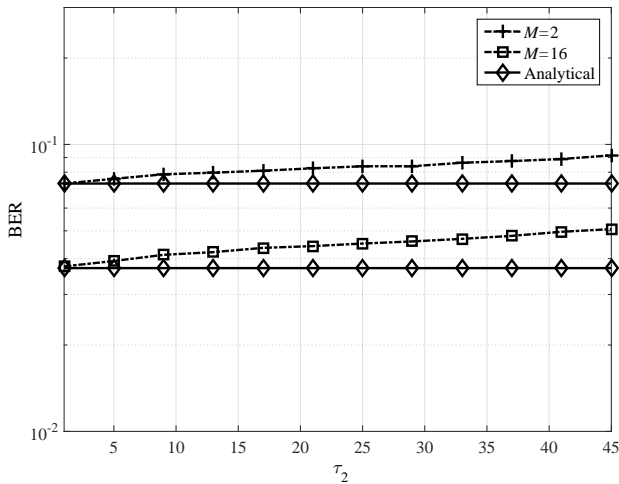Fig. 10: The influence of β on PI-DCSK performance for $M = 4$ and $N_u = 3, 6$ over AWGN channel.

Fig. 8: The BER performance of PI-DCSK for CM1 versus τ_2, for $\beta = 200$, $E_b/N_0 = 16$ dB and $M = 2, 16$.
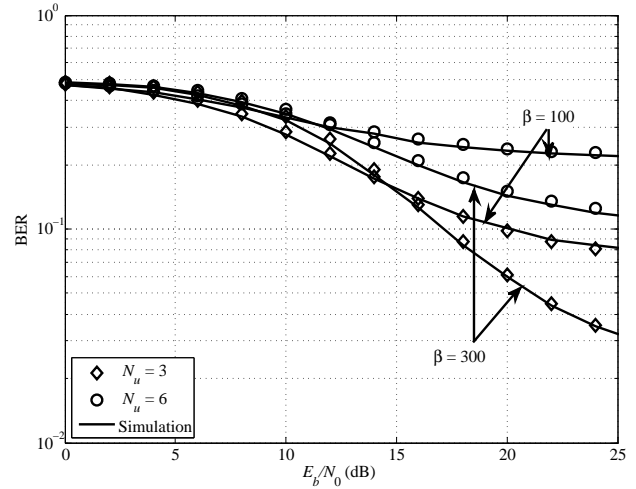

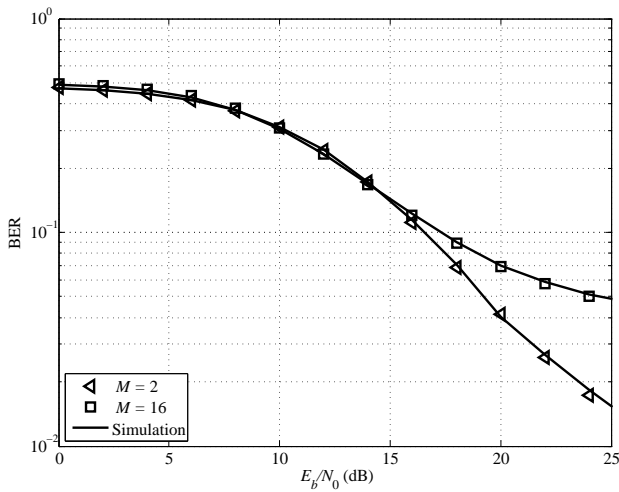Fig. 11: The influence of β on PI-DCSK performance for $M = 4$ and $N_u = 3, 6$ over CM2 channel.

Fig. 9: The influence of modulation order on PI-DCSK performance for $M = 2, 16$, $\beta = 300$ and $N_u = 3$ over CM2 channel.
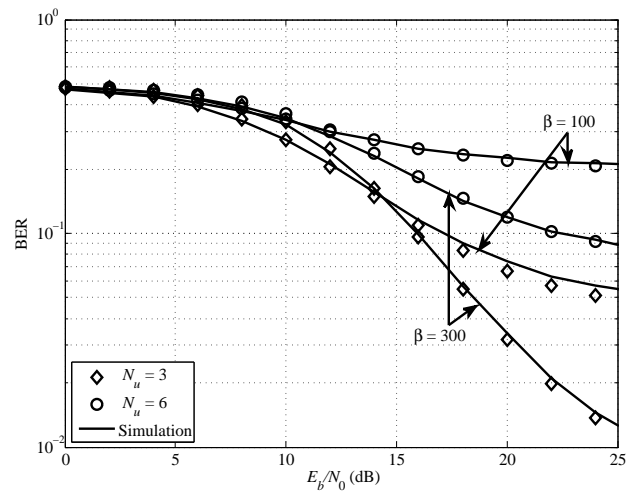

Fig. 12: The influence of β on PI-DCSK performance for $M = 4$ and $N_u = 3, 6$ over CM3 channel.

order to keep MUI noise at an acceptable level, β should be appropriately chosen. Furthermore, as viewed in Figs. 10 and 11, there is a perfect match between analytical and simulation results for both channel models.

In conclusion, the BER performance of the proposed scheme degrades as the number of users increases due to the increment in MUI. Additionally, for the same number of users, the PI-DCSK BER performance worsens as the modulation level increases. However, by increasing the spreading factor, the BER drops and performance improves because the MUI will stretch over a larger bandwidth.

C. Comparison with other non-coherent chaotic modulations

The BER performance of PI-DCSK in comparison with OM-DCSK is evaluated over AWGN, CM1 and CM3 channels. The outcome of this comparison is shown in Fig. 9. This comparison reveals that the BER performance of PI-DCSK and OM-DCSK are approximately similar for $M > 2$, while PI-DCSK significantly outperforms OM-DCSK for $M = 2$ for all channel models. For instance, PI-DCSK needs 2 dB less at the receiver in order to achieve a BER of $= 10^{-3}$ compared to OM-DCSK over an AWGN channel.

In addition, in comparison with PI-DCSK, the BER performance of OM-DCSK significantly degrades over the timely dispersed channel i.e. CM3. This is a consequence of the higher number of correlators at the receiver for the same modulation level M and a loss of orthogonality between different Walsh codes used to construct the orthogonal signal basis. Furthermore, the proposed PI-DCSK achieves the observed BER improvement while sustaining a reduced complexity in comparison to OM-DCSK, as was stated in Section II.

In Fig. 14, the BER performance comparison of PI-DCSK is extended to include DCSK, HE-DCSK and QCSK over AWGN, CM2 and CM3 channels. The PI-DCSK modulation order M is set to 4 and 8. Fig. 14 reveals that at a BER of $= 10^{-3}$, the DCSK BER performance is about 0.8 dB worse than HE-DCSK, QCSK and 4-ary PI-DCSK, and about 2 dB worse than 8-ary PI-DCSK. However, over CM2, the 4-ary PI-DCSK shows a better performance compared to DCSK while it performs slightly worse in comparison to HE-DCSK and QCSK. Furthermore, for $M = 8$, PI-DCSK performance significantly augments, i.e. BER drops due to the mapping of an extra bit in the permutation index, compared to HE-DCSK and QCSK.

D. Discussion

In the proposed PI-DCSK design, multiple quasi-orthogonal sequences are easily generated by virtue of the low auto-correlation properties of the permuted replicas of chaotic sequences.
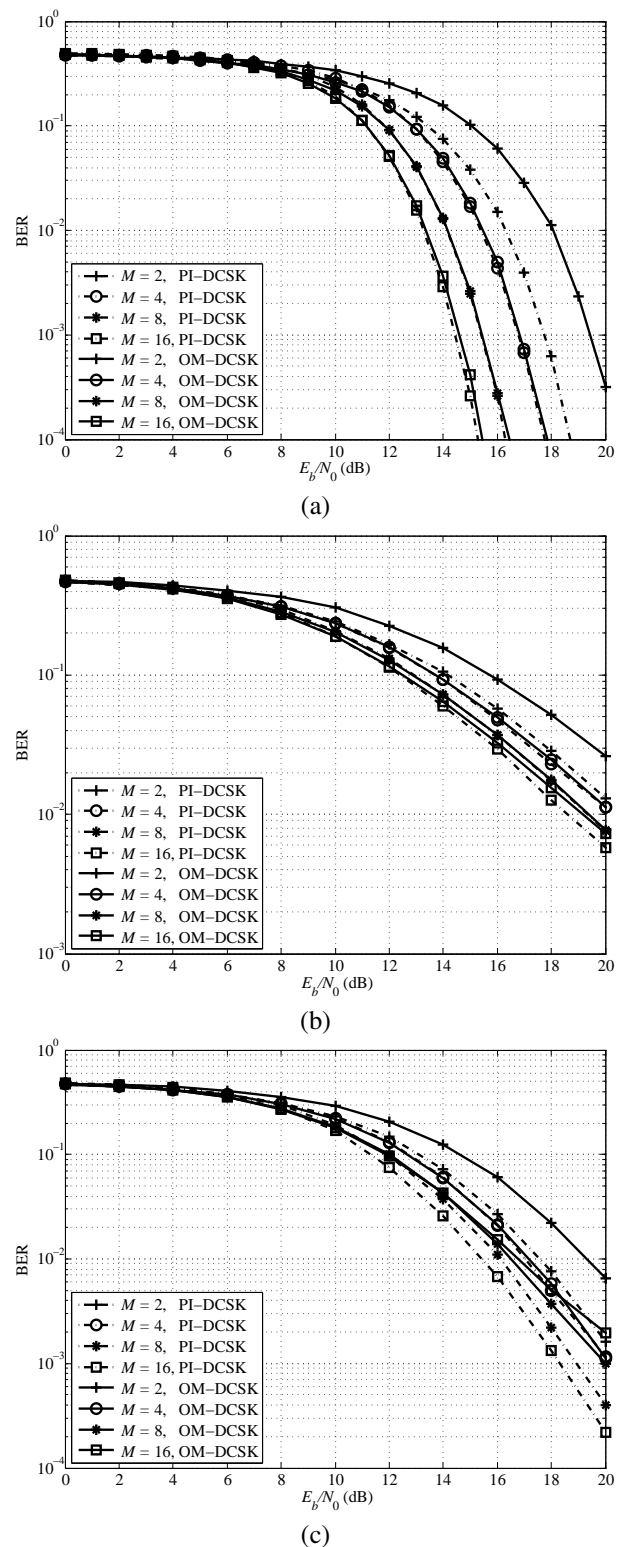

Fig. 13: A BER performance comparison of PI-DCSK to OM-DCSK over (a) AWGN channels for $\beta = 256$, (b) CM1 and (c) CM3 channels with $\beta = 128$.

Therefore, no extra hardware, neither for Hilbert transform nor for the generation of Walsh codes is needed in PI-DCSK in comparison to similar multilevel modulations like OM-DCSK. Moreover, dispensing with the usage of Walsh codes at the receiver, the PI-DCSK scheme enjoys full properties

and advantages of non-coherent modulation. Furthermore, by mapping an extra bit into the permutation indices, the PI-DCSK data rate, BER performance, energy and spectral efficiencies are significantly improved compared to other rival modulation schemes.

VI. CONCLUSIONS

In this paper, a new multi-user multi-level non-coherent PI-DCSK scheme is proposed and analysed for chaos-based communication systems. In the proposed design, time-multiplexing is used to separate reference and data bearing sequences, as in conventional DCSK. In the PI-DCSK scheme presented here, multiple quasi-orthogonal data sequences are formed as a consequence of permuting the reference sequence. In particular, a block of n bits is mapped in the indices of different permutations, where each of the 2^n possible permutations denotes a distinguishable permutation applied to the reference sequence. In completion, the modulated bit is spread by the *selected* permuted reference signal. As multiple bits per data frame are ferried through the use of indexing, the PI-DCSK energy and spectral efficiencies are significantly boosted compared to its competitors.

In addition, the utilisation of different permutations eradicates the similarity between reference sequences and data bearing sequences, which in turn significantly increases the PI-DCSK transmitted data security. Moreover, an efficient multiple access method is proposed for adoption in the PI-DCSK system, by granting absolute access to a distinct set of $M/2$ permutations out of $\beta! - 1$ possible, for each user.

Furthermore, closed-form theoretical expressions of multi-user PI-DCSK system BER over AWGN and multipath Rayleigh channels are derived. Monte-Carlo simulation is used to validate the theoretical results obtained in this work.

In continuation, the influence of different system parameters like modulation orders and spreading sequence lengths are analysed. At the end, the BER performance comparison with DCSK, HE-DCSK, QCSK and OM-DCSK is shown. In light of the obtained results, the proposed novel PI-DCSK system is expected to be competitive and is promising.

REFERENCES

[1] F. C. M. Lau and C. K. Tse, *Chaos-Based Digital communication systems*. Springer-Verlag, 2003.

[2] H. Dedieu and M. P. Kennedy, "Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronization Chua's circuit," *IEEE Trans. Circuits Syst. II, Analog. Digit. Signal Process.*, vol. 40, pp. 634–642, 1993.

[3] C. Rushforth, "Transmitted-reference techniques for random or unknown channels," *IEEE Trans. on Inf. Theory*, vol. 10, no. 1, pp. 39–42, 1964.

[4] G. Kolumbán, G. K. Vizvari, W. Schwarz, and A. Abel, "Differential chaos shift keying: a robust coding for chaos communication," in *Proc. NDES*, Seville, Spain, 1996, pp. 92–97.

[5] G. Kolumbán, G. Kis, M. Kennedy, and Z. Jáko, "FM-DCSK: A new and robust solution to chaos communications," in *Proc. Int. Symp. Nonlinear Theory Appl.*, 1997, pp. 117–120.

[6] W. Xu, L. Wang, and G. Kolumbán, "A novel differential chaos shift keying modulation scheme," *Int. J. Bifurcation Chaos*, vol. 21, no. 03, pp. 799–814, 2011.

[7] H. Yang and G.-P. Jiang, "High-efficiency differential-chaos-shift-keying scheme for chaos-based noncoherent communication," *IEEE Trans. Circuits Syst. II: Exp. Briefs*, vol. 59, no. 5, pp. 312 –316, May 2012.

[8] ——, "Reference-modulated DCSK: a novel chaotic communication scheme," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 60, no. 4, pp. 232–236, 2013.
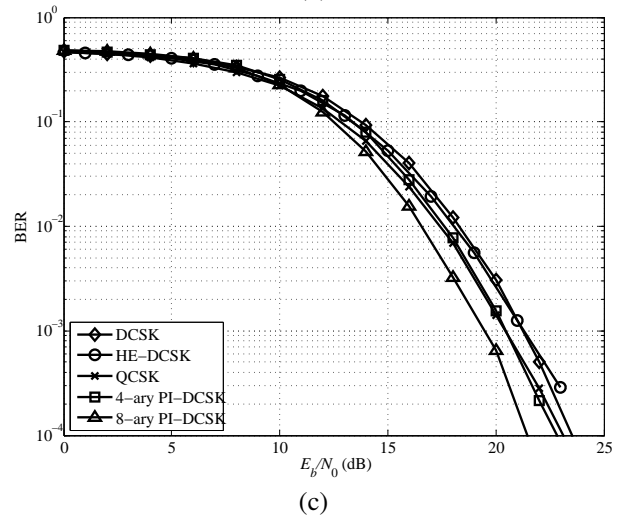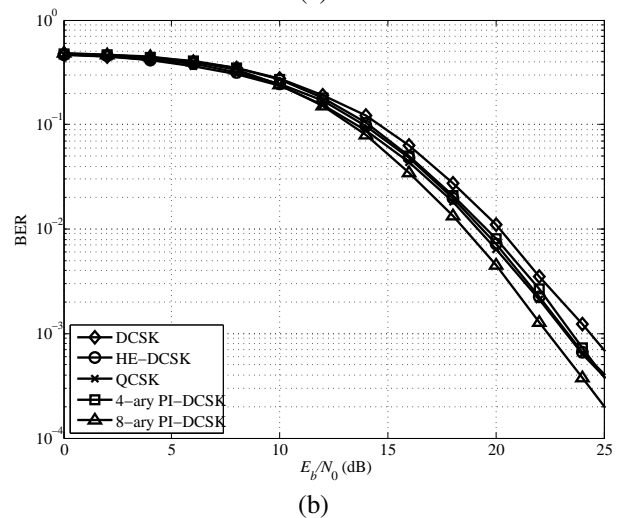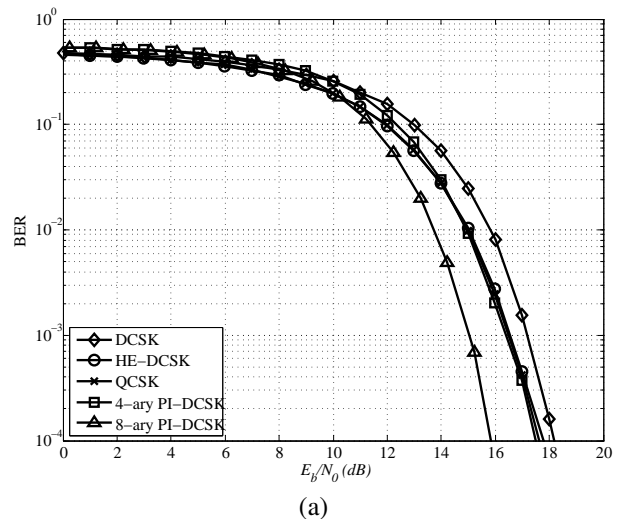
Fig. 14: A BER performance comparison of PI-DCSK to DCSK, HE-DCSK and QCSK for $M = 4$, 8 and $\beta = 200$ in (a) AWGN, (b) CM2 and (c) CM3 channels.

[9] G. Kaddoum and E. Soujeri, "NR-DCSK: A noise reduction differential chaos shift keying system," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 63, no. 7, pp. 648–652, 2016.

[10] G. Kaddoum, E. Soujeri, and Y. Nijsure, "Design of a short reference noncoherent chaos-based communication systems," *IEEE Trans. Com-*

mun., vol. 64, no. 2, pp. 680–689, Feb. 2016.

[11] Z. Galias and G. M. Maggio, "Quadrature chaos-shift keying: theory and performance analysis," *IEEE Trans. Circuits Syst. I: Fundam. Theory Appl.*, vol. 48, no. 12, pp. 1510–1519, Dec. 2001.

[12] F. C. M. Lau and C. K. Tse, "Methods and systems for transceiving chaotic signals," *US Patent No. US7593531, 2009*, 2009.

[13] P. Chen, L. Wang, and F. C. M. Lau, "One analog stbc-dcsk transmission scheme not requiring channel state information," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 60, no. 4, pp. 1027–1037, April 2013.

[14] G. Kaddoum, E. Soujeri, C. Arcila, and K. Eshteiwi, "I-DCSK: An improved non-coherent communication system architecture," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 62, no. 9, pp. 901–905, 2015.

[15] W. Xu, L. Wang, and G. Kolumbán, "A new data rate adaption communications scheme for code-shifted differential chaos shift keying modulation," *Int. J. Bifurcation Chaos*, vol. 22, no. 08, pp. 1–8, 2012.

[16] T. Huang, L. Wang, W. Xu, and F. C. M. Lau, "Multilevel code-shifted differential-chaos-shift-keying system," *IET Commun.*, vol. 10, no. 10, pp. 1189–1195, 2016.

[17] G. Kaddoum and F. Gagnon, "Design of a high-data-rate differential chaos-shift keying system," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 59, no. 7, pp. 448–452, 2012.

[18] Y. Fang, G. Han, P. Chen, F. C. M. Lau, G. Chen, and L. Wang, "A survey on dcsk-based communication systems and their application to uwb scenarios," *IEEE Commun. Surv. Tut.*, vol. 18, no. 3, pp. 1804–1837, thirdquarter 2016.

[19] P. Chen, Y. Fang, G. Han, and G. Chen, "An efficient transmission scheme for dcsk cooperative communication over multipath fading channels," *IEEE Access*, vol. 4, pp. 6364–6373, 2016.

[20] G. Kaddoum, F. Richardson, and F. Gagnon, "Design and analysis of a multi-carrier differential chaos shift keying communication system," *IEEE Trans. Commun.*, vol. 61, no. 8, pp. 3281–3291, Aug. 2013.

[21] G. Cheng, L. Wang, W. Xu, and G. Chen, "Carrier index differential chaos shift keying modulation," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. PP, no. 99, pp. 1–1, 2016.

[22] G. Kaddoum, "Design and performance analysis of a multiuser OFDM based differential chaos shift keying communication system," *IEEE Trans. Commun.*, vol. 64, no. 1, pp. 249–260, 2016.

[23] M. Herceg, K. Miličević, and T. Matić, "Frequency-translated differential chaos shift keying for chaos-based communications," *J. Franklin Inst.*, vol. 353, no. 13, pp. 2966–2979, 2016.

[24] H. Yang, W. K. Tang, G. Chen, and G.-P. Jiang, "System design and performance analysis of orthogonal multi-level differential chaos shift keying modulation scheme," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 63, no. 1, pp. 146–156, 2016.

[25] F. C. M. Lau, K. Y. Cheong, and C. K. Tse, "Permutation-based dcsk and multiple-access dcsk systems," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl*, vol. 50, no. 6, pp. 733–742, June 2003.

[26] Y. Xia, C. Tse, and F. C. Lau, "Performance of differential chaos-shift-keying digital communication systems over a multipath fading channel with delay spread," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 51, no. 12, pp. 680–684, 2004.

[27] J. Daemen and V. Rijme, *The Design of RijndaeL: AES - The Advanced Encryption Standard (Information Security and Cryptography)*. Springer-Verlag Berlin Heidelberg, 2002.

[28] G. Kaddoum, P. Chargé, D. Roviras, and D. Fournier-Prunaret, "A methodology for bit error rate prediction in chaos-based communication systems," *Birkhäuser, Circuits, Syst.Signal Process.*, vol. 28, pp. 925–944, Aug. 2009.

[29] M. Sushchik, L. S. Tsimring, and A. R. Volkovskii, "Performance analysis of correlation-based communication schemes utilizing chaos," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 47, no. 12, pp. 1684–1691, 2000.

[30] G. Kaddoum, Y. Nijsure, and H. Tran, "Generalized code index modulation technique for high-data-rate communication systems," *IEEE Trans. Veh. Technol.*, vol. 65, no. 9, pp. 7000–7009, Sept 2016.

[31] J. G. Proakis, *Digital communications systems*. McGraw-Hill, New York, 2001.

[32] Z. Zhou, T. Zhou, and J. Wang, "Performance of multi-user dcsk communication system over multipath fading channels," in *2007 IEEE International Symposium on Circuits and Systems*, May 2007, pp. 2478–2481.

[33] A. Papoulis, *Probability, Random Variables, and Stochastic Processes*. McGraw-Hill, 1991.

Marijan Herceg (M'14) received the B.Sc. and Ph.D. degrees in Electrical Engineering from the Faculty of Electrical Engineering, Computer Science and Information Technology Osijek, Croatia, in 2002 and 2010, respectively. He is currently an Associate Professor at the Department of Communications, Faculty of Electrical Engineering, Computer Science and Information Technology Osijek, Croatia. His research interests include advanced modulation techniques for impulse radio ultra-wideband (IR-UWB) systems and chaos-based communication systems, multiple access techniques and sigma-delta A/D converters.

Georges Kaddoum (M'11) received the Bachelor's degree in electrical engineering from the Ecole Nationale Supérieure de Techniques Avancées (ENSTA Bretagne), Brest, France, and the M.S. degree in telecommunications and signal processing (circuits, systems, and signal processing) from the Université de Bretagne Occidentale and Telecom Bretagne (ENSTB), Brest, in 2005 and the Ph.D. degree (with honors) in signal processing and telecommunications from the National Institute of Applied Sciences (INSA), University of Toulouse, Toulouse, France, in 2009. Since November 2013, he has been an Assistant Professor of electrical engineering with the Ecole de Technologie Supérieure (ÉTS), University of Quebec, and Montréal, QC, Canada. In 2014, he was awarded the ÉTS Research Chair in physical-layer security for wireless networks. Since 2010, he has been a Scientific Consultant in the field of space and wireless telecommunications for several US and Canadian companies. In 2014, he was awarded the ÉTS Research Chair in physical layer security for wireless networks. He has published over 130+ journal and conference papers and has two pending patents. His recent research activities cover mobile communication systems, modulations, security, and space communications and navigation. Dr. Kaddoum received the Best Papers Awards at the 2014 IEEE International Conference on Wireless and Mobile Computing, Networking, Communications (WIMOB), with three coauthors, and at the 2017 IEEE International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), with four coauthors. Moreover, he honored the 2015 and 2017 IEEE Transactions on Communications Exemplary Reviewer Award. Prof. Kaddoum is currently serving as an Associate Editor for IEEE Transactions on Information Forensics and Security, and IEEE Communications Letters.

Denis Vranješ (M'13) Denis Vranješ received the B.Sc., M.Sc. and Ph.D. degrees in Electrical Engineering from the Faculty of Electrical Engineering, Computer Science and Information Technology Osijek, Croatia in 2008, 2010, and 2016 respectively. Currently, he is a senior instructor at the Department of Communications, Faculty of Electrical Engineering, Computer Science and Information Technology Osijek, Croatia. His research interests are video processing, quality evaluation and wireless communication systems.

Ebrahim Soujeri (M'03, SM'11) received received the B.Sc., M.Sc. and Ph.D. degrees in electrical and electronics engineering from Eastern Mediterranean University (EMU), Famagusta, Northern Cyprus in 1995, 1997 and 2003, respectively. He has been pursuing his second Ph.D. at École de Technologie Suprieure (ÉTS), Montréal, QC, Canada, since September 2014. He was with the Department of Electrical and Electronics Engineering, EMU, from 1996 to 2002, as a Research Assistant while pursuing the M.Sc. and Ph.D. degrees. In 2002, he taught in the department of computer engineering at Cyprus International University for one year. In 2003, he joined the Faculty of Engineering, European University of Lefke in Northern Cyprus. In 2007, he was a Visiting Assistant Professor at Sultan Qaboos University, Muscat, Oman. Dr. Soujeri has also taught in the department of computer science and software engineering at Concordia University, Montreal, Canada on part-time basis in 2012-2014. His research interests include wireless communication systems, spread spectrum, and index modulation techniques. He is a reviewer of various IEEE journals and conferences.