A Spectrum-Efficient M-ary Correlation Delay Shift Keying Scheme for Non-coherent Chaotic Communications

Xiangming Cai, Weikai Xu, Shaohua Hong, Lin Wang
Dept. of Information and Communication Engineering, Xiamen University, Fujian 361005, China
Email:xweikai@xmu.edu.cn

2021 15th International Symposium on Medical Information and Communication Technology (ISMICT) | 978-1-7281-7724-3/20/$31.00 ©2021 IEEE | DOI: 10.1109/ISMICT51748.2021.9434939

***Abstract*—Considering the signal structure of a differential chaos shift keying (DCSK) scheme, the reference and information-bearing signals are transmitted sequentially, thereby increasing the probability of being detected by a malicious eavesdropper and degrading the system security. Against this background, a spectrum-efficient M-ary correlation delay shift keying (M-ary CDSK) scheme is proposed in this paper, where a digital signal processing technique, namely QR decomposition, is applied to different chaotic signals to cancel the intrasignal interference completely. The M-ary CDSK scheme can not only improve the system security by embedding the reference signal into the M-ary information-bearing signal, but also achieve better spectral efficiency by M-ary modulation. The analytical bit error rate (BER) expressions are derived to verify the validness of the proposed scheme. Simulation results indicate that the M-ary CDSK scheme is capable of obtaining 1 to 4dB performance gain better than other schemes and providing a reliable solution for non-coherent chaotic communications.**

***Index Terms*—Chaotic communications, correlation delay shift keying, QR decomposition, M-ary modulation, spectral efficiency.**

I. Introduction

Chaotic signals, by virtue of their wideband characteristics, are naturally suitable for spread-spectrum (SS) communications, which spread narrowband information over a wide frequency spectrum to harvest the benefits of jamming resistance and low probability of interception (LPI) [1]. Therefore, chaotic communications, using chaotic signals as the spread-spectrum carriers have received increasing considerations over the past few decades [2], [3]. A non-coherent differential chaos shift keying (DCSK) scheme shows good robustness against the fading channel without the need for complex chaos synchronization and channel estimation [4]. In the DCSK scheme, a reference chaotic signal is first transmitted in the first half of the symbol duration, followed by a modulated chaotic signal. Note that the transmitted-reference structure of the DCSK scheme makes this scheme spectrum-inefficient. On the other hand, the sequential transmission of reference and information-bearing signals in the DCSK scheme increases the probability of being detected by a malicious eavesdropper, therefore degrading the system security [5].

Against this background, a correlation delay shift keying (CDSK) scheme was proposed in [6], where the reference and information-bearing signals are overlapped together with a certain delay, making the malicious detection difficult. More importantly, the CDSK scheme can achieve double spectral efficiency compared to the DCSK scheme, as no individual reference signal is sent by a slot. Motivated by this paradigm, the authors of [7] proposed a generalized CDSK (GCDSK) scheme, where multiple reference and information-bearing signals are transmitted within the same time slot and therefore the transmitted signal is more homogeneous and less prone to interception. Since the reference signal and its delayed version modulated by a modulated symbol are transmitted in an overlapping manner, the intrasignal interference becomes more dominant in the CDSK and GCDSK schemes when a correlation receiver is used. Therefore, there is a compelling interest in the research community to improve the BER performance of the CDSK scheme. For example, a repeated CDSK (R-CDSK) scheme was proposed in [8], where a CDSK symbol is transmitted first and followed by a differential version, enhancing the BER performance. Moreover, a reference-adaptive CDSK (RA-CDSK) scheme was proposed in [9] to decrease the intrasignal interference of the GCDSK scheme. A phase-orthogonality CDSK (PO-CDSK) scheme [10] obtains better BER performance than the GCDSK scheme, because the PO-CDSK scheme introduces the quadrature sinusoidal wavelets to eliminate the intrasignal interference between the reference and information-bearing signals.

The aforementioned CDSK-based schemes are based on a binary constellation, which restricts the further improvement of spectral efficiency. Since the chaotic signal and its delayed version are not strictly orthogonal, a great amount of intrasignal interference is involved in the CDSK scheme, degrading the system performance. Against this background, a spectrum-efficient M-ary correlation delay shift keying (M-ary CDSK) scheme is presented in this paper, where QR decomposition [11] is applied to different chaotic signals to cancel the intrasignal interference completely. Moreover, an M-ary constellation is used in the M-ary CDSK scheme and therefore the M-ary CDSK scheme can improve the spectral efficiency by adjusting constellation parameters. The main contributions of this paper are (1) An M-ary correlation delay shift keying (M-ary CDSK) scheme is proposed to provide a spectrum-efficient and reliable solution for non-coherent chaotic communications. (2) The BER expressions of the M-

ary CDSK scheme are derived over additive white Gaussian noise (AWGN) and multipath Rayleigh fading channels. Then, the correctness of our derivations is validated by computer simulations. (3) After performing computer simulations and making contrast with other non-coherent chaotic communication schemes, it is clearly demonstrated that the M-ary CDSK scheme can achieve 1 to 4dB performance gain.

The remainder of this paper is structured as follow. Section II shows the system model of the M-ary CDSK scheme. Performance analysis is given in Section III. In Section IV, computer simulations are performed for the M-ary CDSK scheme. Finally, Section V concludes this paper.

II. M-ARY CDSK SCHEME

A. The Transmitter

Fig. 1 shows the block diagram of the M-ary CDSK scheme. Since the chaotic signal has the sensitive characteristic depending on the initial condition and the properties of a delta-function-like self-correlation and low cross-correlation, it is easy to generate N uncorrelated chaotic signals by a chaos generator with N different initial values. Define the obtained N chaotic signals as $\{\mathbf{x}_1, \mathbf{x}_2, \cdots, \mathbf{x}_N\}$, where $\mathbf{x}_i = [x_{i,1}, x_{i,2}, \cdots, x_{i,\beta}]^T, i \in \{1, 2, \cdots, N\}$ is a β-length chaotic signal generated by a 2-order Chebyshev map. β is the spreading factor, and $[\cdot]^T$ is the transposition operation. Generally, $N = 8$ is used in the M-ary CDSK scheme.

Then, QR decomposition is performed for the resultant N chaotic signals to obtain the orthogonal and normalized chaotic signals. According to [11], QR decomposition indicates that $\mathbf{A} = \mathbf{QR}$ decomposes the matrix $\mathbf{A}$ into $\mathbf{Q}$ and $\mathbf{R}$, in which $\mathbf{Q}$ is an orthonormal matrix and $\mathbf{R}$ is an upper triangular matrix. Specifically, for simplicity, a 4×4 matrix $\mathbf{A}$ is used to explain the process of QR decomposition[1]. The first column vector $\mathbf{a}_1$ is normalized to obtain

$$r_{1,1} = \|\mathbf{a}_1\| = \sqrt{(a_{1,1})^2 + (a_{2,1})^2 + (a_{3,1})^2 + (a_{4,1})^2}, \quad (1)$$

then $\{r_{12}, r_{13}, r_{14}\}$ can be computed by

$$\begin{aligned} r_{1,j} =& (\mathbf{q}_1)^T \mathbf{a}_j \\ =& q_{1,1}a_{1,j} + q_{2,1}a_{2,j} + q_{3,1}a_{3,j} + q_{4,1}a_{4,j}, j \in \{2, 3, 4\}, \end{aligned} \quad (2)$$

where $\mathbf{q}_1 = \frac{\mathbf{a}_1}{r_{1,1}}$, i.e.,

$$q_{1,1} = \frac{a_{1,1}}{r_{1,1}}, q_{2,1} = \frac{a_{2,1}}{r_{1,1}}, q_{3,1} = \frac{a_{3,1}}{r_{1,1}}, q_{4,1} = \frac{a_{4,1}}{r_{1,1}}. \quad (3)$$

Therefore, we obtain the first column vectors of $\mathbf{Q}$ and $\mathbf{R}$. After that, the next iterative matrix $\mathbf{A}^1$ can be defined as $\mathbf{A}^1 = [\mathbf{a}_1^1, \mathbf{a}_2^1, \mathbf{a}_3^1, \mathbf{a}_4^1]$, where $\mathbf{a}_1^1 = 0$, $\mathbf{a}_2^1 = \mathbf{a}_2 - r_{1,2}\mathbf{q}_1$, $\mathbf{a}_3^1 = \mathbf{a}_3 - r_{1,3}\mathbf{q}_1$ and $\mathbf{a}_4^1 = \mathbf{a}_4 - r_{1,4}\mathbf{q}_1$. Similarly, the above-mentioned operations are performed again based on $\mathbf{A}^1$, i.e.,

$$r_{2,2} = \|\mathbf{a}_2^1\| = \sqrt{(a_{1,2}^1)^2 + (a_{2,2}^1)^2 + (a_{3,2}^1)^2 + (a_{4,2}^1)^2}, \quad (4)$$

$$\mathbf{q}_2 = \frac{\mathbf{a}_2^1}{r_{2,2}}, \quad (5)$$

[1]Notation: $a_{i,j}$ is row and column of the matrix $\mathbf{A}$, and $\mathbf{a}_j$ is the column vector of the matrix $\mathbf{A}$. $\|\cdot\|$ denotes the norm operation.

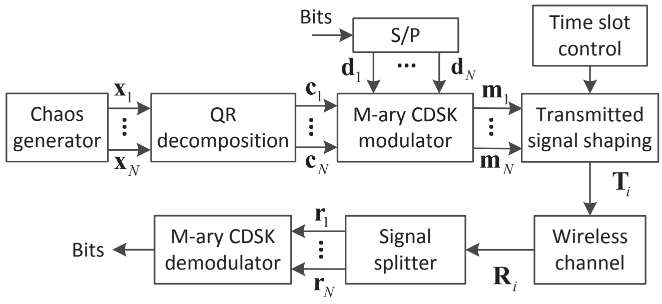

Fig. 1. Block diagram of the M-ary CDSK scheme.

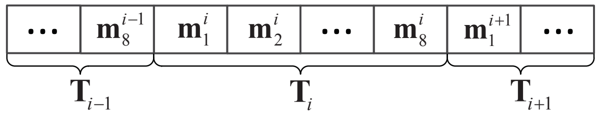

Fig. 2. Frame format of the transmitted signal for the M-ary CDSK scheme.

$$r_{2,j} = (\mathbf{q}_2)^T \mathbf{a}_j^1, j \in \{3, 4\}. \quad (6)$$

With the aid of (4), (5) and (6), the column vectors of the matrix $\mathbf{A}^2$ can be calculated as $\mathbf{a}_1^2 = 0$, $\mathbf{a}_2^2 = 0$, $\mathbf{a}_3^2 = \mathbf{a}_3^1 - r_{2,3}\mathbf{q}_2$ and $\mathbf{a}_4^2 = \mathbf{a}_4^1 - r_{2,4}\mathbf{q}_2$. Continuing to carry out the aforementioned operations, we obtain the orthonormal matrix $\mathbf{Q}$ and the upper triangular matrix $\mathbf{R}$, respectively, given as

$$\mathbf{Q} = \begin{bmatrix} q_{1,1} & q_{1,2} & q_{1,3} & q_{1,4} \\ q_{2,1} & q_{2,2} & q_{2,3} & q_{2,4} \\ q_{3,1} & q_{3,2} & q_{3,3} & q_{3,4} \\ q_{4,1} & q_{4,2} & q_{4,3} & q_{4,4} \end{bmatrix}, \quad (7)$$

$$\mathbf{R} = \begin{bmatrix} r_{1,1} & r_{1,2} & r_{1,3} & r_{1,4} \\ 0 & r_{2,2} & r_{2,3} & r_{2,4} \\ 0 & 0 & r_{3,3} & r_{3,4} \\ 0 & 0 & 0 & r_{4,4} \end{bmatrix}. \quad (8)$$

As shown in Fig. 1, after being processed by the block of QR decomposition, N chaotic signals $\{\mathbf{x}_1, \mathbf{x}_2, \cdots, \mathbf{x}_N\}$ are converted into their orthonormal versions $\{\mathbf{c}_1, \mathbf{c}_2, \cdots, \mathbf{c}_N\}$. Subsequently, the resultant signals and information bits are loaded into the M-ary CDSK modulator to form the transmitted signal. Fig. 2. shows the frame format of the transmitted signal for the M-ary CDSK scheme. Particularly, for each transmitted frame, there are $N = 8$ M-ary CDSK symbols used to carry $8n$ information bits. The modulation order of the M-ary CDSK scheme is $M = 2^n$, where n is the total number of transmitted bits per M-ary CDSK symbol. The overall transmitted bits per M-ary CDSK frame can be represented in a vector form as $\{\mathbf{d}_1, \mathbf{d}_2, \cdots, \mathbf{d}_N\}$, where $\mathbf{d}_k = \{d_1, d_2, \cdots, d_n\}, k \in \{1, 2, \cdots, N\}$ is the information bits transmitted in the k^{th} M-ary CDSK symbol. After converting the information bits $\mathbf{d}_k$ into an M-ary constellation symbol $s_k = s_k^R + \sqrt{-1}s_k^I$, the M-ary information-bearing signal is given as $s_k^R\mathbf{c}_i + s_k^I\mathbf{c}_j$, where s_k^R and s_k^I are real and imaginary parts of the M-ary symbol s_k. Table I gives a pattern of frame format for the M-ary CDSK scheme. Note that this signal format is not available for the eavesdropper.

TABLE I
THE SIGNAL STRUCTURE OF THE M-CDSK SCHEME WITH $N=8$

Sequence number	Transmitted signal	Reference signal	Information-bearing signal
1	$\mathbf{m}_1=\mathbf{c}_1+s_1^R\mathbf{c}_2+s_1^I\mathbf{c}_3$	$\mathbf{c}_1$	$s_1^R\mathbf{c}_2+s_1^I\mathbf{c}_3$
2	$\mathbf{m}_2=\mathbf{c}_2+s_2^R\mathbf{c}_4+s_2^I\mathbf{c}_5$	$\mathbf{c}_2$	$s_2^R\mathbf{c}_4+s_2^I\mathbf{c}_5$
3	$\mathbf{m}_3=\mathbf{c}_3+s_3^R\mathbf{c}_6+s_3^I\mathbf{c}_7$	$\mathbf{c}_3$	$s_3^R\mathbf{c}_6+s_3^I\mathbf{c}_7$
4	$\mathbf{m}_4=\mathbf{c}_4+s_4^R\mathbf{c}_1+s_4^I\mathbf{c}_6$	$\mathbf{c}_4$	$s_4^R\mathbf{c}_1+s_4^I\mathbf{c}_6$
5	$\mathbf{m}_5=\mathbf{c}_5+s_5^R\mathbf{c}_1+s_5^I\mathbf{c}_7$	$\mathbf{c}_5$	$s_5^R\mathbf{c}_1+s_5^I\mathbf{c}_7$
6	$\mathbf{m}_6=\mathbf{c}_6+s_6^R\mathbf{c}_2+s_6^I\mathbf{c}_8$	$\mathbf{c}_6$	$s_6^R\mathbf{c}_2+s_6^I\mathbf{c}_8$
7	$\mathbf{m}_7=\mathbf{c}_7+s_7^R\mathbf{c}_2+s_7^I\mathbf{c}_8$	$\mathbf{c}_7$	$s_7^R\mathbf{c}_2+s_7^I\mathbf{c}_8$
8	$\mathbf{m}_8=\mathbf{c}_8+s_8^R\mathbf{c}_3+s_8^I\mathbf{c}_4$	$\mathbf{c}_8$	$s_8^R\mathbf{c}_3+s_8^I\mathbf{c}_4$

Therefore, considering the i^{th} signal frame, the transmitted signal of the M-ary CDSK scheme can be expressed as

$$\mathbf{T}_i=\begin{bmatrix}\mathbf{m}_1^i\\ \mathbf{m}_2^i\\ \vdots\\ \mathbf{m}_8^i\end{bmatrix}^T. \tag{9}$$

B. The Receiver

Considering a widely used L-path Rayleigh fading channel, the channel coefficient and time delay of the l^{th} path are given as α_l and τ_l, respectively. When the transmitted signal is contaminated by the Rayleigh fading channel and additive white Gaussian noise, the received signal can be obtained by

$$\mathbf{R}_i=\sum\nolimits_{l=1}^{L}\alpha_l\mathbf{T}_{i,\tau_l}+\mathbf{n}_i, \tag{10}$$

where L is the number of paths and $\mathbf{n}_i$ is an AWGN vector with zero mean and $N_0/2$ variance. It is assumed that the channel delay τ_l is much shorter than the spreading factor β so that the inter-symbol interference (ISI) is ignorable. For simplification, the subscripts i and τ_l are omitted in the sequel. At the receiver, the received signal is first split to obtain different M-ary CDSK symbols, given as $\mathbf{r}_j=\mathbf{R}_i[(j-1)\beta+1:j\beta]$, where $\mathbf{R}_i[(j-1)\beta+1:j\beta]$ is the $\{(j-1)\beta+1\}^{th}$ to $\{j\beta\}^{th}$ element of $\mathbf{R}_i$. According to the signal structure of the M-ary CDSK scheme as shown in Table I, since the N chaotic signals are independent and orthogonal to each other, the reference signals embedded in different M-ary CDSK symbols can be fully utilized to demodulate the information bits. For example, the references signals of the second and third M-ary CDSK symbols are used to retrieve the information bits carried by the first M-ary CDSK symbol. Therefore, the second and third M-ary CDSK symbols are correlated with the first M-ary CDSK symbols to obtain the in-phase and quadrature decision variables, formulated as

$$\begin{aligned}Z_1^I&=\left(\sum\nolimits_{l=1}^{L}\alpha_l\mathbf{m}_1+\mathbf{n}_1\right)^T\left(\sum\nolimits_{l=1}^{L}\alpha_l\mathbf{m}_2+\mathbf{n}_2\right)\\&=\left[\sum\nolimits_{l=1}^{L}\alpha_l\left(\mathbf{c}_1+s_1^R\mathbf{c}_2+s_1^I\mathbf{c}_3\right)+\mathbf{n}_1\right]^T\\&\quad\times\left[\sum\nolimits_{l=1}^{L}\alpha_l\left(\mathbf{c}_2+s_2^R\mathbf{c}_4+s_2^I\mathbf{c}_5\right)+\mathbf{n}_2\right],\end{aligned} \tag{11}$$

$$\begin{aligned}Z_1^Q&=\left(\sum\nolimits_{l=1}^{L}\alpha_l\mathbf{m}_1+\mathbf{n}_1\right)^T\left(\sum\nolimits_{l=1}^{L}\alpha_l\mathbf{m}_3+\mathbf{n}_3\right)\\&=\left[\sum\nolimits_{l=1}^{L}\alpha_l\left(\mathbf{c}_1+s_1^R\mathbf{c}_2+s_1^I\mathbf{c}_3\right)+\mathbf{n}_1\right]^T\\&\quad\times\left[\sum\nolimits_{l=1}^{L}\alpha_l\left(\mathbf{c}_3+s_3^R\mathbf{c}_6+s_3^I\mathbf{c}_7\right)+\mathbf{n}_3\right].\end{aligned} \tag{12}$$

Afterwards, the transmitted M-ary constellation symbol can be estimated by

$$\hat{s}_1=\arg\underbrace{\min}_{s\in S}\left(\left|\left(Z_1^I+\sqrt{-1}Z_1^Q\right)-s\right|^2\right), \tag{13}$$

where S is the set of M-ary constellation symbols. Finally, after converting the estimated M-ary constellation symbol into binary bits, the receiver recovers the information bits $\mathbf{d}_1$. The in-phase and quadrature decision variables of other M-ary CDSK symbols are enumerated in Table II. Similarly, other information bits $\{\mathbf{d}_2,\mathbf{d}_3,\cdots,\mathbf{d}_N\}$ can be restored by the aforementioned operations.

III. PERFORMANCE ANALYSIS

In this section, the BER expressions of the propsoed M-ary CDSK scheme are derived over AWGN and multipth Rayleigh fading channels. The M-ary CDSK symbols within a frame are independent of each other and they have similar signal structure so that the first one is evaluated for brevity. Considering the first M-ary CDSK symbol, the in-phase and quadrature decision variables Z_1^I and Z_1^Q can be simplified as (14) and (15), as shown at the bottom of next page. U_1 and V_1 are the useful components. U_2 and V_2 are the terms of noise interference, while U_3 and V_3 are the terms of intrasignal

TABLE II

THE IN-PAHSE AND QUADRATURE DECISION VARIABLES OF DIFFERENT M-ARY CDSK SYMBOLS

Sequence number	In-phase decision variable	Quadrature decision variable
1	$Z_1^I = (\sum_{l=1}^L \alpha_l \mathbf{m}_1 + \mathbf{n}_1)^T (\sum_{l=1}^L \alpha_l \mathbf{m}_2 + \mathbf{n}_2)$	$Z_1^Q = (\sum_{l=1}^L \alpha_l \mathbf{m}_1 + \mathbf{n}_1)^T (\sum_{l=1}^L \alpha_l \mathbf{m}_3 + \mathbf{n}_3)$
2	$Z_2^I = (\sum_{l=1}^L \alpha_l \mathbf{m}_2 + \mathbf{n}_2)^T (\sum_{l=1}^L \alpha_l \mathbf{m}_4 + \mathbf{n}_4)$	$Z_2^Q = (\sum_{l=1}^L \alpha_l \mathbf{m}_2 + \mathbf{n}_2)^T (\sum_{l=1}^L \alpha_l \mathbf{m}_5 + \mathbf{n}_5)$
3	$Z_3^I = (\sum_{l=1}^L \alpha_l \mathbf{m}_3 + \mathbf{n}_3)^T (\sum_{l=1}^L \alpha_l \mathbf{m}_6 + \mathbf{n}_6)$	$Z_3^Q = (\sum_{l=1}^L \alpha_l \mathbf{m}_3 + \mathbf{n}_3)^T (\sum_{l=1}^L \alpha_l \mathbf{m}_7 + \mathbf{n}_7)$
4	$Z_4^I = (\sum_{l=1}^L \alpha_l \mathbf{m}_4 + \mathbf{n}_4)^T (\sum_{l=1}^L \alpha_l \mathbf{m}_1 + \mathbf{n}_1)$	$Z_4^Q = (\sum_{l=1}^L \alpha_l \mathbf{m}_4 + \mathbf{n}_4)^T (\sum_{l=1}^L \alpha_l \mathbf{m}_6 + \mathbf{n}_6)$
5	$Z_5^I = (\sum_{l=1}^L \alpha_l \mathbf{m}_5 + \mathbf{n}_5)^T (\sum_{l=1}^L \alpha_l \mathbf{m}_1 + \mathbf{n}_1)$	$Z_5^Q = (\sum_{l=1}^L \alpha_l \mathbf{m}_5 + \mathbf{n}_5)^T (\sum_{l=1}^L \alpha_l \mathbf{m}_7 + \mathbf{n}_7)$
6	$Z_6^I = (\sum_{l=1}^L \alpha_l \mathbf{m}_6 + \mathbf{n}_6)^T (\sum_{l=1}^L \alpha_l \mathbf{m}_2 + \mathbf{n}_2)$	$Z_6^Q = (\sum_{l=1}^L \alpha_l \mathbf{m}_6 + \mathbf{n}_6)^T (\sum_{l=1}^L \alpha_l \mathbf{m}_8 + \mathbf{n}_8)$
7	$Z_7^I = (\sum_{l=1}^L \alpha_l \mathbf{m}_7 + \mathbf{n}_7)^T (\sum_{l=1}^L \alpha_l \mathbf{m}_2 + \mathbf{n}_2)$	$Z_7^Q = (\sum_{l=1}^L \alpha_l \mathbf{m}_7 + \mathbf{n}_7)^T (\sum_{l=1}^L \alpha_l \mathbf{m}_8 + \mathbf{n}_8)$
8	$Z_8^I = (\sum_{l=1}^L \alpha_l \mathbf{m}_8 + \mathbf{n}_8)^T (\sum_{l=1}^L \alpha_l \mathbf{m}_3 + \mathbf{n}_3)$	$Z_8^Q = (\sum_{l=1}^L \alpha_l \mathbf{m}_8 + \mathbf{n}_8)^T (\sum_{l=1}^L \alpha_l \mathbf{m}_4 + \mathbf{n}_4)$

interference. Since the chaotic signals $\{\mathbf{c}_1, \mathbf{c}_2, \cdots, \mathbf{c}_8\}$ are orthonormal to each other, i.e., $(\mathbf{c}_i)^T \mathbf{c}_j = 1$ when $i = j$ and $(\mathbf{c}_i)^T \mathbf{c}_j = 0$ when $i \neq j$, the terms of intrasignal interference are zero. Therefore, the mean and variance of the decision variable Z_1^I are calculated as

$$\mathrm{E}\left[Z_1^I\right] = \sum\nolimits_{l=1}^{L} \alpha_l^2 s_1^R \frac{nE_b}{2}, \tag{16}$$

$$\mathrm{Var}\left[Z_1^I\right] = \sum\nolimits_{l=1}^{L} \alpha_l^2 n E_b N_0 + \beta \frac{N_0^2}{4}, \tag{17}$$

where $\mathrm{E}[\cdot]$ and $\mathrm{Var}[\cdot]$ are the expectation and variance operations, respectively. In addition, $E_b = 2\mathrm{E}[(\mathbf{c}_i)^T \mathbf{c}_i]/n$ is the bit energy of the proposed M-ary CDSK scheme. Since the in-phase and quadrature decision variables Z_1^I and Z_1^Q are symmetric, the mean and variance of Z_1^Q are given as $\mathrm{E}[Z_1^Q] = \sum_{l=1}^L \alpha_l^2 s_1^I \frac{nE_b}{2}$ and $\mathrm{Var}[Z_1^Q] = \sum_{l=1}^L \alpha_l^2 n E_b N_0 + \beta \frac{N_0^2}{4}$, respectively. Therefore, the BER of the proposed M-ary CDSK scheme can be approximately computed by [12], [13]

$$P_e \approx \frac{1}{n}\left[1 - \int_{-\frac{\pi}{M}}^{\frac{\pi}{M}} \frac{1}{2\pi} \exp\left(-\frac{\rho^2}{2}\right) + \exp\left(-\frac{\rho^2 \sin^2\psi}{2}\right) \times \frac{\rho\cos\psi}{\sqrt{2\pi}} Q(-\rho\cos\psi) \mathrm{d}\psi\right], \tag{18}$$

where $\rho = \frac{\mathrm{E}[Z_1^I]}{s_1^R \sqrt{\mathrm{Var}[Z_1^I]}} = \frac{n\gamma_b}{\sqrt{4n\gamma_b + \beta}}$ and $\gamma_b = \sum_{l=1}^L \alpha_l^2 \frac{E_b}{N_0}$ is the signal-to-noise ratio (SNR). In addition, $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^{+\infty} \exp(-\frac{t^2}{2}) \mathrm{d}t, x \geq 0$.

In this paper, an L-paths independent and identically distributed (i.i.d.) Rayleigh fading channel is used. According to [14], the instantaneous SNR α_l follows an exponential distribution, namely $f(\alpha_l) = \frac{1}{\bar{\alpha}_l} \exp(-\frac{\alpha_l}{\bar{\alpha}_l}), l \in \{1, 2, \cdots, L\}$, where $\bar{\alpha}_l = \frac{E_b}{N_0} \mathrm{E}[\alpha_l^2]$ denotes the averaged SNR of the l^{th}

$$\begin{aligned} Z_1^I =& \left[\sum_{l=1}^{L} \alpha_l \left(\mathbf{c}_1 + s_1^R \mathbf{c}_2 + s_1^I \mathbf{c}_3\right) + \mathbf{n}_1\right]^T \left[\sum_{l=1}^{L} \alpha_l \left(\mathbf{c}_2 + s_2^R \mathbf{c}_4 + s_2^I \mathbf{c}_5\right) + \mathbf{n}_2\right] \\ =& \underbrace{\sum_{l=1}^{L} \alpha_l^2 s_1^R (\mathbf{c}_2)^T \mathbf{c}_2}_{U_1} + \underbrace{\sum_{l=1}^{L} \alpha_l \left(\mathbf{c}_2 + s_2^R \mathbf{c}_4 + s_2^I \mathbf{c}_5\right)^T \mathbf{n}_1 + \sum_{l=1}^{L} \alpha_l \left(s_1^R \mathbf{c}_2 + s_1^I \mathbf{c}_3 + \mathbf{c}_1\right)^T \mathbf{n}_2 + (\mathbf{n}_1)^T \mathbf{n}_2}_{U_2} \\ &+ \underbrace{\sum_{l=1}^{L} \alpha_l^2 \left[(\mathbf{c}_1)^T \mathbf{c}_2 + s_2^R (\mathbf{c}_1)^T \mathbf{c}_4 + s_2^I (\mathbf{c}_1)^T \mathbf{c}_5 + s_1^R s_2^R \mathbf{c}_2 (\mathbf{c}_4)^T + s_1^R s_2^I \mathbf{c}_2 (\mathbf{c}_5) + s_1^I (\mathbf{c}_3)^T \mathbf{c}_2 + s_1^I s_2^R (\mathbf{c}_3)^T \mathbf{c}_4 + s_1^I s_2^I (\mathbf{c}_3)^T \mathbf{c}_5\right]}_{U_3 = 0}, \end{aligned} \tag{14}$$

$$\begin{aligned} Z_1^Q =& \left[\sum_{l=1}^{L} \alpha_l \left(\mathbf{c}_1 + s_1^R \mathbf{c}_2 + s_1^I \mathbf{c}_3\right) + \mathbf{n}_1\right]^T \left[\sum_{l=1}^{L} \alpha_l \left(\mathbf{c}_3 + s_3^R \mathbf{c}_6 + s_3^I \mathbf{c}_7\right) + \mathbf{n}_3\right] \\ =& \underbrace{\sum_{l=1}^{L} \alpha_l^2 s_1^I (\mathbf{c}_3)^T \mathbf{c}_3}_{V_1} + \underbrace{\sum_{l=1}^{L} \alpha_l \left(\mathbf{c}_3 + s_3^R \mathbf{c}_6 + s_3^I \mathbf{c}_7\right)^T \mathbf{n}_1 + \sum_{l=1}^{L} \alpha_l \left(\mathbf{c}_1 + s_1^R \mathbf{c}_2 + s_1^I \mathbf{c}_3\right)^T \mathbf{n}_3 + (\mathbf{n}_1)^T \mathbf{n}_3}_{V_2} \\ &+ \underbrace{\sum_{l=1}^{L} \alpha_l^2 \left[(\mathbf{c}_1)^T \mathbf{c}_3 + s_3^R (\mathbf{c}_1)^T \mathbf{c}_6 + s_3^I (\mathbf{c}_1)^T \mathbf{c}_7 + s_1^R (\mathbf{c}_2)^T \mathbf{c}_3 + s_1^R s_3^R (\mathbf{c}_2)^T \mathbf{c}_6 + s_1^R s_3^I (\mathbf{c}_2)^T \mathbf{c}_7 + s_1^I s_3^R (\mathbf{c}_3)^T \mathbf{c}_6 + s_1^I s_3^I (\mathbf{c}_3)^T \mathbf{c}_7\right]}_{V_3 = 0}. \end{aligned} \tag{15}$$

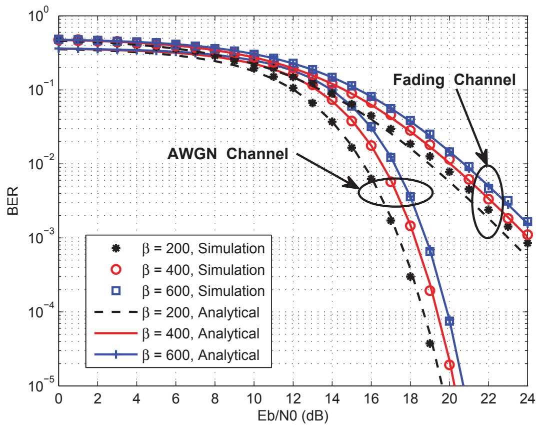

Fig. 3. BER performance of the M-ary CDSK scheme with $M = 4$ and $\beta = 200, 400, 600$ over AWGN and multipath Rayleigh fading channels.

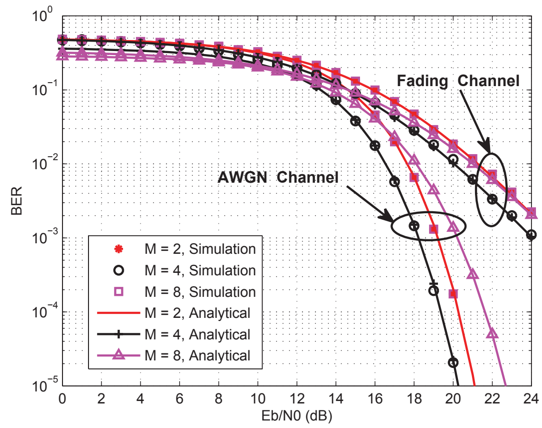

Fig. 4. BER performance of the M-ary CDSK scheme with $M = 2, 4, 8$ and $\beta = 400$ over AWGN and multipath Rayleigh fading channels.

path. Therefore, the bit error probability of the proposed M-ary CDSK scheme is obtained by [15]

$$P_{\text{fading}} = \int_0^{+\infty} \cdots \int_0^{+\infty} \int_0^{+\infty} P_e(\gamma_b | \gamma_b = \sum_{l=1}^{L} \gamma_l) \times \prod_{l=1}^{L} \frac{1}{\bar{\gamma}_l} \exp\left(-\frac{\gamma_l}{\bar{\gamma}_l}\right) \mathrm{d}\gamma_1 \mathrm{d}\gamma_2 \cdots \mathrm{d}\gamma_L. \tag{19}$$

IV. Numerical Results and Discussions

In this section, the spectral efficiency and BER performance of the M-ary CDSK scheme are evaluated to confirm the effectiveness of the proposed scheme. Unless specific statement, a three-paths Rayleigh fading channel with equal channel coefficients and channel delays $\tau_1 = 0, \tau_2 = 1, \tau_3 = 3$ is applied in simulations. The spectral efficiency is defined as the ratio of bit rate to total bandwidth in bits/s/Hz [16]. It is assumed that the bandwidth of subcarrier is B. Therefore, the spectral efficiency of the M-ary CDSK scheme is calculated as $\aleph_1 = \frac{n}{\beta T_c B}$. According to [12], [17], the spectral efficiency of the M-ary DCSK and GCS-MDCSK schemes are $\aleph_2 = \frac{n}{2\beta T_c B}$ and $\aleph_3 = \frac{U_t n}{N \beta T_c B}$, respectively, where U_t is total number of parallel information-bearing signals and its maximum is $(N-2)/2$. Therefore, it can be seen that the spectral efficiency of the M-ary CDSK scheme is twice and over twice as good as the M-ary DCSK and GCS-MDCSK schemes, respectively.

The BER performance of the M-ary CDSK scheme with different spreading factors is plotted in Fig. 3. It is clearly shown that the analytical results are in a good agreement with the theoretical ones. On the other hand, when the spreading factor β increases from 200 to 600, the BER performance of the M-ary CDSK scheme degrades, which is due to the increasing contribution of noise-noise cross terms in (14) and (15). Furthermore, the effect of M on the BER performance of the M-ary CDSK scheme is studied in Fig. 4. Clearly, the analytical curves accord with the simulated ones, validating the correctness of our derivations in Section III. As observed in Fig. 4, the M-ary CDSK scheme with $M = 4$ is capable of obtaining more than 2dB performance gain better than that of $M = 8$. Although the M-ary CDSK scheme with $M = 2$ achieves about 1.5dB performance gain over $M = 8$ in the AWGN channel, the M-ary CDSK scheme with $M = 8$ is slightly better than that of $M = 2$ in the fading channel.

The BER performance of the M-ary CDSK, M-ary DCSK [12] and GCS-MDCSK [17] schemes with same spectral

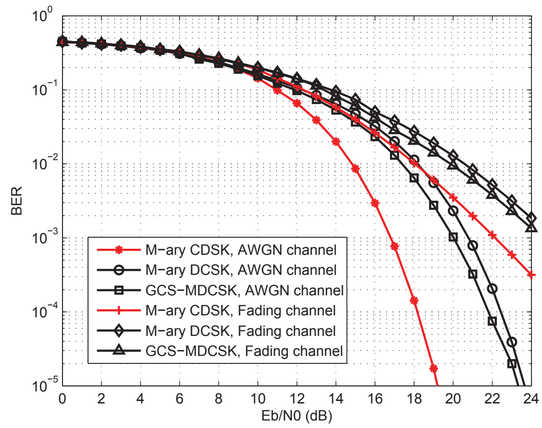

Fig. 5. BER performance of the M-ary CDSK, M-ary DCSK and GCS-MDCSK schemes over AWGN and multipath Rayleigh fading channels under the condition of same spectral efficiency.

TABLE III
SIMULATION PARAMETERS

Scheme	β	n	Spectral efficiency†
M-ary CDSK	100	2	$\aleph_1 = \frac{n}{\beta T_c B} = 0.02$
M-ary DCSK	100	4	$\aleph_2 = \frac{n}{2\beta T_c B} = 0.02$
GCS-MDCSK	50	4	$\aleph_3 = \frac{U_t}{N \beta T_c B} = 0.02$

† It is assumed that $BT_c = 1$. Moreover, $U_t = 1$ and $N = 4$ is used for the GCS-MDCSK scheme.

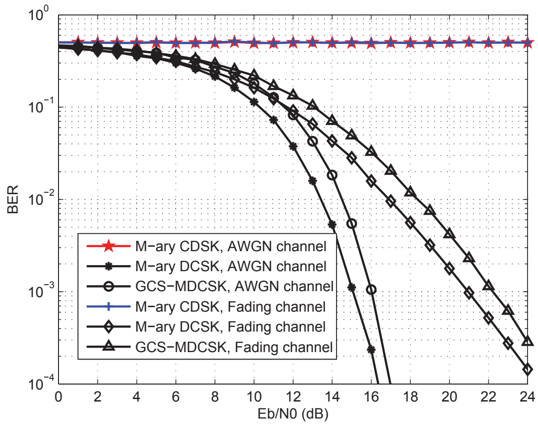

Fig. 6. BER performance of the eavesdropper under the condition of different signal formats. $\beta = 100$ and $M = 4$.

efficiency is plotted in Fig. 5. In the GCS-MDCSK scheme, $U_t = 1$ and the order of Walsh codes is 4. Other simulation parameters are given in Table III and the spectral efficiency of different systems is also shown in this table. As can be seen from Fig. 5, the BER performance of the proposed M-ary CDSK scheme is capable of achieving about 4dB performance gain over that of the GCS-MDCSK scheme at the BER level of 10^{-5} in the AWGN channel. Moreover, in the fading channel, the performance gap between M-ary CDSK and GCS-MDCSK schemes is about 2dB at the BER of 10^{-3}.

When two users use the signal formats of M-ary CDSK, M-ary DCSK and GCS-MDCSK schemes for communications, the BER performance of a malicious eavesdropper is evaluated in Fig. 6. Assuming that Walsh codes and a correlation receiver are available for the eavesdropper. As observed, the illegal user can not eavesdrop the information when the signal format of the M-ary CDSK scheme is used for communications, because the illegal user has high BER (almost 0.5) in the case of M-ary CDSK signal format. In contrast, when the signal formats of M-ary DCSK and GCS-MDCSK schemes are used, it is easy for the eavesdropper to intercept the information, which threatens the system security. Therefore, the proposed M-ary CDSK scheme shows strong anti-interception performance.

V. Conclusion

In this paper, a novel M-ary correlation delay shift keying (M-ary CDSK) scheme has been proposed to improve the spectral efficiency and system security of non-coherent chaotic communication schemes. In the M-ary CDSK, the overlapping transmission of reference and information-bearing signals makes the information bits undetectable for a malicious eavesdropper, thereby strengthening the system security. In addition, compared to the DCSK scheme, the proposed M-ary CDSK scheme does not use additional time slot to transmit the reference signal, thus enhancing the spectral efficiency. Moreover, a QR decomposition algorithm is applied to chaotic signals so that the adverse effect of intrasignal interference is eliminated significantly. The analytical BER expressions are also given to validate the effectiveness of the proposed M-ary CDSK scheme. Finally, substantial simulations demonstrate that in the case of same spectral efficiency, the M-ary CDSK scheme achieves 1 to 4dB performance gain better than other non-coherent chaotic communication schemes. Furthermore, the M-ary CDSK scheme also shows superior anti-interception performance against eavesdropping.

Acknowledgement

This work was supported in part by the Natural Science Foundation (NSF) of China under Grant No. 61871337 and 61671395, in part by the NSF of Fujian Province under Grant No. 2020J01003 and in part by the NSF of Guangdong Province under Grant No. 2018A030313710.

References

[1] 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. Survey Tutor.*, vol. 18, no. 3, pp. 1804-1837, third quarter 2016.

[2] M. Qian, G. Cai, Y. Fang and G. Han, "Design of link-selection strategies for buffer-aided DCSK-SWIPT relay system," *IEEE Trans. Commun.*, vol. 68, no. 10, pp. 6023-6038, Oct. 2020.

[3] G. Cai, Y. Fang, P. Chen, G. Han, G. Cai and Y. Song, "Design of an MISO-SWIPT-aided code-index modulated multi-carrier M-DCSK system for e-Health IoT," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 2, pp. 311-324, Feb. 2021.

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

[5] G. Kaddoum, "Wireless chaos-based communication systems: A comprehensive survey," *IEEE Access*, vol. 4, pp. 2621-2648, 2016.

[6] 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, Dec. 2000.

[7] W. M. Tam, F. C. M. Lau and C. K. Tse, "Generalized correlation-delay-shift-keying scheme for noncoherent chaos-based communication systems," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 53, no. 3, pp. 712-721, March 2006.

[8] J. Shen, W. Rao, W. Zhang, L. Zhang and Z. Wu, "An improved repeated correlation delay shift keying modulation scheme for chaotic communication system," in *2015 ICCC*, Shenzhen, 2015, pp. 1-5.

[9] J. Duan, G. Jiang and H. Yang, "Reference-adaptive CDSK: An enhanced version of correlation delay shift keying," *IEEE Trans. Circuits Syst. II, Exp. Briefs.*, vol. 62, no. 1, pp. 90-94, Jan. 2015.

[10] J. Duan and H. Yang, "Phase-orthogonality CDSK: A reliable and effective chaotic communication scheme," *IET Commun.*, vol. 12, no. 9, pp. 1116-1122, 5 6 2018.

[11] L. N. Trefethen and D. Bau, *Numerical Linear Algebra*. Philadelphia, PA: SIAM, 1997.

[12] L. Wang, G. Cai and G. R. Chen, "Design and performance analysis of a new multiresolution M-ary differential chaos shift keying communication system," *IEEE Trans. Wireless Commun.*, vol. 14, no. 9, pp. 5197-5208, Sept. 2015.

[13] X. Cai, W. Xu, D. Wang, S. Hong and L. Wang, "An M-ary orthogonal multilevel differential chaos shift keying system with code index modulation," *IEEE Trans. Commun.*, vol. 67, no. 7, pp. 4835-4847, July 2019.

[14] J. G. Proakis and M. Salehi, *Digital Communications*. New York, NY, USA: McGraw-Hill, 2007.

[15] M. K. Simon and M.-S. Alouini, *Digital Communication Over Fading Channels*, vol. 95, 2nd ed. Newark, NJ, USA: Wiley, 2005.

[16] X. Cai, W. Xu, L. Wang and G. Kolumbán, "Multicarrier M-ary orthogonal chaotic vector shift keying with index modulation for high data rate transmission," *IEEE Trans. Commun.*, vol. 68, no. 2, pp. 974-986, Feb. 2020.

[17] Y. Tan, W. Xu and S. Hong, "An M-ary code shifted differential chaos shift keying scheme," in *2017 23rd APCC*, Perth, WA, 2017, pp. 1-6.