Generalized Correlation-Delay-Shift-Keying Scheme for Noncoherent Chaos-Based Communication Systems

Wai M. Tam, Francis C. M. Lau, *Senior Member, IEEE*, and Chi K. Tse, *Fellow, IEEE*

***Abstract*—In this paper, we propose a generalized correlation-delay-shift-keying (GCDSK) scheme for noncoherent chaos-based communications. In the proposed scheme, several delayed versions of a chaotic signal are first produced. Some of them will be modulated by the binary data to be transmitted. The delayed signals will then be added to the original chaotic signal and transmitted. At the receiver, a simple correlator-type detector is employed to decode the binary symbols. The approximate bit error rate (BER) of the GCDSK scheme is derived analytically based on Gaussian approximation. Simulations are performed and compared with the noncoherent correlation-delay-shift-keying (CDSK) and differential chaos-shift-keying (DCSK) modulation schemes. The effects of the spreading factor, length of delay, and the number of delay units on the BER are fully studied. It is found that GCDSK can achieve better BER performance than DCSK under reasonable bit-energy-to-noise-power-spectral-density ratios.**

***Index Terms*—Chaos communications, correlation-delay-shift-keying, noncoherent communications.**

I. Introduction

WHEN a narrow-band signal modulates a wide-band carrier, the signal bandwidth will be increased substantially. Also, the power spectral density (psd) will be lowered accordingly without affecting the bit error performance. Because of the low psd, the signal can be hidden under the background noise, thus guaranteeing a low probability of detection by unintended parties. In addition, the wide signal bandwidth can provide antijamming capabilities when appropriate demodulation techniques are applied. Such features, namely, low probability of detection and antijamming, are typical characteristics possessed by spread-spectrum communication systems [1].

Recently, chaotic signals, having a wide-band nature, have been proposed as carriers for spread-spectrum communications. A number of coherent systems have been suggested and studied [2]–[5]. For a coherent system, an exact replica of the chaotic signal needs to be reproduced at the receiving end. Because robust synchronization techniques are yet to be developed, coherent systems are still not realizable in a practical environment [6].

Noncoherent communication schemes, which do not require the reproduction of the chaotic signals at the receiving end, are more feasible in practice. The first noncoherent chaos-based digital communication scheme, namely, *differential chaos-shift-keying* (DCSK) scheme, was proposed by Kolumbán *et al.* [7]. In DCSK, a reference chaotic signal is sent, followed by the same signal modulated by a binary symbol. At the receiver, these two pieces of chaotic signals are correlated. The binary symbol is then decoded based on the sign of the correlator output [5]–[9]. Another noncoherent detection technique, which is applicable to *chaos-shift-keying* (CSK) modulation scheme, has been proposed by Hasler and Schimming [10]. The technique is based on an optimal classifier which optimizes the bit error rate (BER) by selecting the symbol that minimizes the *a posteriori* probabilities. The computational complexity of the classifier is further studied by Lau and Tse [11], and an approximate-optimal detection scheme is then proposed [12]. In addition, Tse *et al.* have reported another noncoherent detector for CSK [13]. The detection principles are formulated on the reconstruction of the return map of the chaotic signals and the regression method.

Besides the aforementioned basic noncoherent detection schemes, a number of DCSK-based derivatives have evolved to further enhance the DCSK scheme. For example, *frequency-modulated DCSK* (FM-DCSK) has been proposed to overcome the varying bit-energy problem in DCSK [14], [15]. Instead of feeding a chaotic signal into a DCSK modulator, the chaotic signal is applied to modulate the frequency of a sinusoidal carrier, producing a chaotic FM signal. By sending the chaotic FM signal to a DCSK modulator, an FM-DCSK output is produced which has a constant amplitude, and hence constant power and energy per bit duration. *Quadrature CSK* (QCSK), a multilevel version of DCSK, has been investigated by Galias and Maggio [16]. Based upon the generation of an orthogonal of chaotic functions, QCSK allows an increase in data rate with respect to DCSK, with the same bandwidth occupation. In the DCSK scheme, because of the similarity between the reference and information-bearing chaotic samples, the bit rate of the system can be easily derived. This may not be very desirable if we want to hide the signal away from unintended parties. In the *permutation-based DCSK* (P-DCSK) scheme [17], a permutation transformation is introduced in the modulator to shuffle the chaotic samples, destroying the similarity between the reference and information-bearing samples in the DCSK system. By doing so, the bit rate is made undetectable from the frequency spectrum, thereby enhancing the data security. *Correlation delay-shift-keying* (CDSK) scheme is similar to the DCSK scheme in that a reference chaotic signal is embedded in

Manuscript received July 10, 2003; revised February 27, 2004. This work was supported in part by a Postdoctoral Fellowship provided by The Hong Kong Polytechnic University. This paper was recommended by Associate Editor L. Kocarev.

The authors are with the Department of Electronic and Information Engineering, The Hong Kong Polytechnic University, Hong Kong (e-mail: tamwm@eie.polyu.edu.hk; encmlau@polyu.edu.hk; encktse@polyu.edu.hk).

Digital Object Identifier 10.1109/TCSI.2005.858323

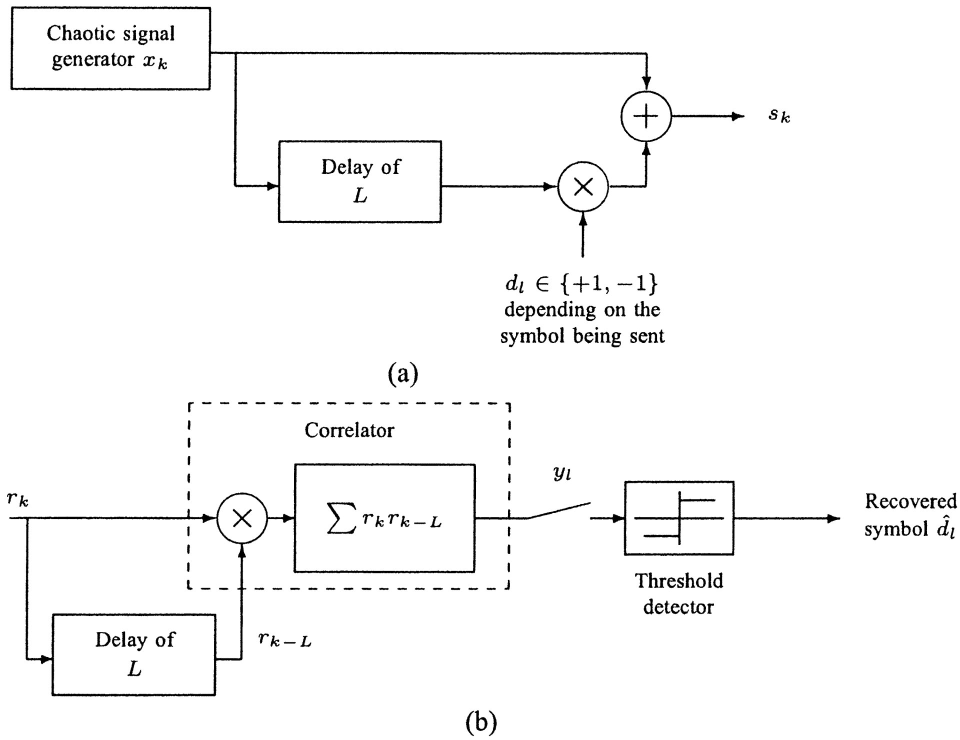

Fig. 1. CDSK system. (a) Transmitter. (b) Receiver.

the transmitted signal [18]. Unlike in DCSK, however, the reference signal and the information-bearing signal are now added together with a certain time delay in CDSK. As a consequence, each transmitted signal sample includes one reference sample and one information-bearing sample, and the transmitted signal sample is never repeated. Since no individual reference signal is sent, the bandwidth efficiency is improved. Moreover, by eliminating the switch required to perform the switching between the reference chaotic signal and information-bearing signal in the DCSK system, CDSK allows a continuous operation of the transmitter. Also, the transmitted signal is more homogeneous and less prone to interception. However, because the sum of two chaotic signals is sent, more uncertainty (interference) is produced when the received signal correlates with its delayed version at the receiving side. Therefore, the performance of CDSK is worse than that of DCSK.

In this paper, we propose a generalized CDSK (GCDSK) scheme. The transmitted signal is composed of a reference chaotic signal and a number of delayed chaotic signals, some of which are modulated by the data being sent. Such a construction of the transmitted signal allows the transmission of more than one reference signal and more than one information-bearing signal simultaneously. The useful signal component, as well as the interference component, will be enhanced at the receiving side. We show that with appropriate choice of system parameters, the bit error performance of the proposed system improves over the CDSK scheme. The system also inherits the merits of the CDSK system such as being switchless and allowing continuous operation of the transmitter. The organization of the paper is as follows. In Section II, the operation of a baseband implementation of the CDSK system is briefly reviewed, and in Section III, the proposed GCDSK scheme is described. Assuming a Gaussian correlator output, an approximate BER is derived analytically in terms of the spreading factor, length of delay and the number of delay units. Finally, using the Chebyshev map as the chaotic generator, we perform simulations for the GCDSK system and present the results in Section IV. Besides comparing with the analytical results, the simulation results for the GCDSK scheme are also compared with those of the DCSK and CDSK schemes.

II. REVIEW OF CDSK SCHEME

Fig. 1 shows the transmitter and receiver structures of a CDSK system [18]. Denote the lth transmitted symbol by $d_l \in \{-1, +1\}$ and assume that "$+1$" and "-1" are transmitted with equal probabilities. First a chaotic signal, denoted by $\{x_k\}$, is generated in the transmitter. The transmitted signal, s_k, is the sum of the chaotic signal x_k and the delayed version of the signal, x_{k-L}, modulated by the symbol $d_l \in \{-1, +1\}$, where L denotes the delay, i.e.,

$$s_k = x_k + d_l x_{k-L}. \tag{1}$$

Denote the spreading factor by β, i.e., β chaotic signals s_k, are sent within one bit duration. Consider the lth transmitted symbol d_l and the transmitted signals related to it. For $k = (l-1)\beta + 1 - L, (l-1)\beta + 2 - L, \ldots, l\beta - L$, the transmitted signal equals

$$s_k = \underbrace{x_k}_{\text{reference signal for the } l\text{th symbol}} + d_\theta x_{k-L} \tag{2}$$

in which the reference signal x_k for the lth symbol is embedded, and d_θ with $\theta \le l$ represents the symbol modulating the delayed

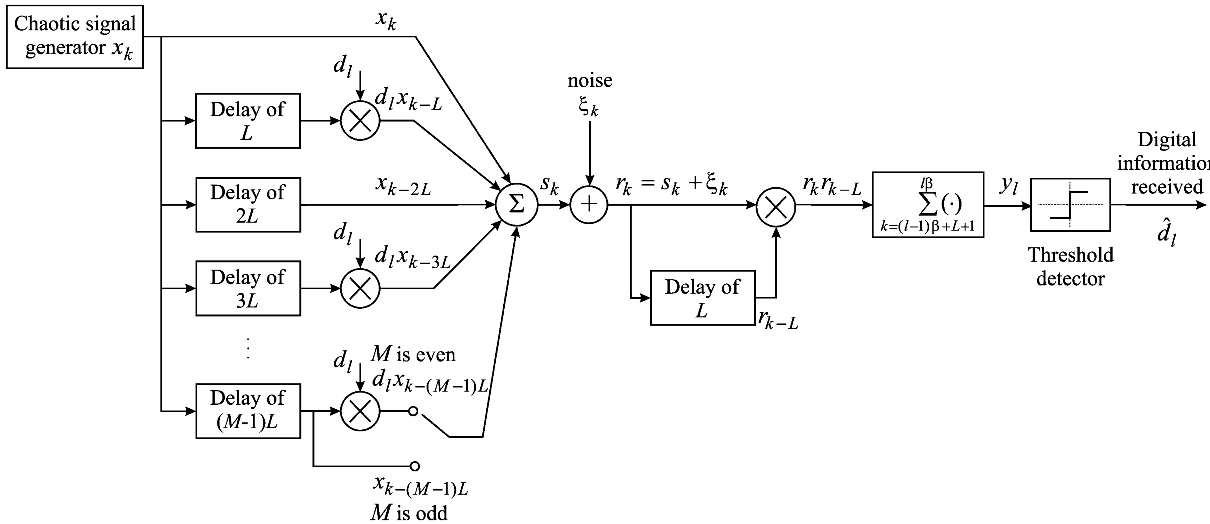

Fig. 2. Block diagram of a generalized CDSK communication system.

chaotic signal component. Further, during the time when $k = (l-1)\beta+1, (l-1)\beta+2, \ldots, l\beta$, the transmitted signal

$$s_k = x_k + \underbrace{d_l x_{k-L}}_{\text{information-bearing signal for the } l\text{th symbol}} \tag{3}$$

now contains the information-bearing part $d_l x_{k-L}$ for the lth symbol. Therefore, by correlating the chaotic signals in these two time intervals, the lth transmitted symbol d_l can be decoded.

Assume that the transmitted signal is passed through an additional white Gaussian noise (AWGN) channel with a two-sided power spectral density $N_0/2$. The received signal, denoted by r_k, is given by

$$r_k = s_k + \xi_k \tag{4}$$

where ξ_k denotes the AWGN signal with zero mean and variance $N_0/2$. At the receiving side, the received signal correlates with an L-sample-delayed version of itself within each symbol duration.

The output of the correlator at the end of the lth symbol duration, denoted by y_l, equals

$$\begin{aligned} y_l &= \sum_{k=(l-1)\beta+1}^{l\beta} r_k r_{k-L} \\ &= \sum_{k=(l-1)\beta+1}^{(l-1)\beta+L-\lfloor \frac{L}{\beta}\rfloor\beta} (x_k + d_l x_{k-L} + \xi_k) \\ &\quad \times \left(x_{k-L} + d_{l-\lfloor \frac{L}{\beta}\rfloor-1} x_{k-2L} + \xi_{k-L}\right) \\ &\quad + \sum_{k=(l-1)\beta+L-\lfloor \frac{L}{\beta}\rfloor\beta+1}^{l\beta} (x_k + d_l x_{k-L} + \xi_k) \\ &\quad \times \left(x_{k-L} + d_{l-\lfloor \frac{L}{\beta}\rfloor} x_{k-2L} + \xi_{k-L}\right) \\ &= \lambda + \mu + \nu \end{aligned} \tag{5}$$

where λ, μ, and ν denote the *required signal*, the *intrasignal interference* and the *noise component*, respectively, and are given by

$$\lambda = d_l \sum_{k=(l-1)\beta+1}^{l\beta} x_{k-L}^2 \tag{6}$$

$$\begin{aligned} \mu = &\sum_{k=(l-1)\beta+1}^{(l-1)\beta+L-\lfloor \frac{L}{\beta}\rfloor\beta} \Big(x_k x_{k-L} + d_{l-\lfloor \frac{L}{\beta}\rfloor-1} x_k x_{k-2L} \\ &+ d_l d_{l-\lfloor \frac{L}{\beta}\rfloor-1} x_{k-L} x_{k-2L}\Big) \\ &+ \sum_{k=(l-1)\beta+L-\lfloor \frac{L}{\beta}\rfloor\beta+1}^{l\beta} (x_k x_{k-L} \\ &+ d_{l-\lfloor \frac{L}{\beta}\rfloor} x_k x_{k-2L} \\ &+ d_l d_{l-\lfloor \frac{L}{\beta}\rfloor} x_{k-L} x_{k-2L}\Big) \end{aligned} \tag{7}$$

$$\begin{aligned} \nu = &\sum_{k=(l-1)\beta+1}^{l\beta} (x_k \xi_{k-L} + d_l x_{k-L} \xi_{k-L} \\ &+ x_{k-L}\xi_k + \xi_k \xi_{k-L}) \\ &+ \sum_{k=(l-1)\beta+1}^{(l-1)\beta+L-\lfloor \frac{L}{\beta}\rfloor\beta} d_{l-\lfloor \frac{L}{\beta}\rfloor-1} x_{k-2L}\xi_k \\ &+ \sum_{k=(l-1)\beta+L-\lfloor \frac{L}{\beta}\rfloor\beta+1}^{l\beta} d_{l-\lfloor \frac{L}{\beta}\rfloor} x_{k-2L}\xi_k. \end{aligned} \tag{8}$$

Note that in the above equations, the function $\lfloor \varsigma \rfloor$ computes the integral part of ς. As in a DCSK system, the required signal in (6) is a time-varying component, depending upon the bit energy of the transmitted signal. The intrasignal interference, similar to the interuser interference in a multiple access system [19], originates from the correlation between the chaotic samples and may contribute positively or negatively to the required signal. The net effect is that more uncertainty on the correlator output is produced. Finally, the noise component comes from the noisy channel. Based on the correlator output, the symbol is decoded according to the following rule

$$\hat{d}_l = \begin{cases} +1, & \text{if } y_l > 0 \\ -1, & \text{if } y_l \leq 0. \end{cases} \tag{9}$$

Because of the additional uncertainty due to the intrasignal interference, the performance of the CDSK system is always lower than that of the DCSK system. In particular, under a noiseless condition, the correlator for the CDSK receiver produces

$$y_l = \lambda + \mu. \tag{10}$$

Under the same condition, the correlator in the DCSK receiver gives only the required signal component, i.e., λ [6]. By comparing these two expressions, we may conclude that DCSK outperforms CDSK in a noiseless environment.

III. GCDSK Scheme

A. Transmitter Structure

We propose a generalized CDSK (GCDSK) communication system, as shown in Fig. 2. The transmitter contains a chaotic signal generator and $(M-1)$ delay blocks. We assume that $M > 2$ because when $M = 2$, the GCDSK system degenerates to the CDSK system. Denote the minimum delay by L. The chaotic signals with delays $L, 3L, 5L, \ldots$ are modulated by the data sequence $\{d_l\}$, whereas the signals with delays $2L, 4L, 6L, \ldots$ are unmodulated. Finally, the transmitted signal is formed by adding the original chaotic signal and all the delayed signals. As in Section II, we define β as the spreading factor, i.e., the number of transmitted signals in each bit duration. During the lth bit duration, i.e., for time $k = (l-1)\beta+1, (l-1)\beta+2, \ldots, l\beta$, the transmitted signal is given by (11), as shown at the bottom of the page, where in each case, the first and second terms represent summation of all the unmodulated and modulated chaotic signals, respectively.

B. Receiver Structure

As in Section II, we assume an AWGN channel and we use a similar correlator-type detector. The only difference in the correlator is that only $(\beta - L)$ terms (assuming $\beta > L$) will be added in the summation block. Although part of the useful signal component will be lost by summing only $(\beta - L)$ terms, the intrasignal interference component will also be reduced because the appearance of the bit value d_{l-1} will be avoided in the received signal for d_l. For the lth symbol, the corresponding output of the correlator equals (12), as shown at the bottom of the page, where

$$\lambda_{\text{even}} = \sum_{k=(l-1)\beta+L+1}^{l\beta} d_l \left(\sum_{m=1}^{\frac{M-2}{2}} x_{k-2mL}^2 + \sum_{m=0}^{\frac{M-2}{2}} x_{k-(2m+1)L}^2 \right) \tag{13}$$

$$\mu_{\text{even}} = \sum_{k=(l-1)\beta+L+1}^{l\beta} \left[\left[\sum_{m=0}^{\frac{M-2}{2}} \left(x_{k-2mL} + d_l x_{k-(2m+1)L} \right) \right] \times \left[\sum_{m=0}^{\frac{M-2}{2}} \left(x_{k-(2m+1)L} + d_l x_{k-(2m+2)L} \right) \right] \right] - \lambda_{\text{even}} \tag{14}$$

$$\nu_{\text{even}} = \sum_{k=(l-1)\beta+L+1}^{l\beta} \left[\sum_{m=0}^{\frac{M-2}{2}} \left(x_{k-2mL} + d_l x_{k-(2m+1)L} \right) \xi_{k-L} + \sum_{m=0}^{\frac{M-2}{2}} \left(x_{k-(2m+1)L} + d_l x_{k-(2m+2)L} \right) \xi_k + \xi_k \xi_{k-L} \right] \tag{15}$$

$$s_k = \begin{cases} \sum_{m=0}^{\frac{M-2}{2}} x_{k-2mL} + d_l \sum_{m=0}^{\frac{M-2}{2}} x_{k-(2m+1)L}, & \text{if } M \text{ is even} \\ \sum_{m=0}^{\frac{M-1}{2}} x_{k-2mL} + d_l \sum_{m=0}^{\frac{M-3}{2}} x_{k-(2m+1)L}, & \text{if } M \text{ is odd} \end{cases} \tag{11}$$

$$\begin{aligned} y_l &= \sum_{k=(l-1)\beta+L+1}^{l\beta} r_k r_{k-L} \\ &= \begin{cases} \sum_{k=(l-1)\beta+L+1}^{l\beta} \left[\left(\sum_{m=0}^{\frac{M-2}{2}} \left(x_{k-2mL} + d_l x_{k-(2m+1)L} \right) + \xi_k \right) \times \left(\sum_{m=0}^{\frac{M-2}{2}} \left(x_{k-(2m+1)L} + d_l x_{k-(2m+2)L} \right) + \xi_{k-L} \right) \right], & \text{if } M \text{ is even} \\ \sum_{k=(l-1)\beta+L+1}^{l\beta} \left[\left(\sum_{m=0}^{\frac{M-1}{2}} x_{k-2mL} + d_l \sum_{m=0}^{\frac{M-3}{2}} x_{k-(2m+1)L} + \xi_k \right) \times \left(\sum_{m=0}^{\frac{M-1}{2}} x_{k-(2m+1)L} + d_l \sum_{m=0}^{\frac{M-3}{2}} x_{k-(2m+2)L} + \xi_{k-L} \right) \right], & \text{if } M \text{is odd} \end{cases} \\ &= \begin{cases} \lambda_{\text{even}} + \mu_{\text{even}} + \nu_{\text{even}}, & \text{if} M \text{ is even} \\ \lambda_{\text{odd}} + \mu_{\text{odd}} + \nu_{\text{odd}}, & \text{if } M \text{ is odd} \end{cases} \end{aligned} \tag{12}$$

$$\lambda_{\text{odd}} = \sum_{k=(l-1)\beta+L+1}^{l\beta} d_l \left(\sum_{m=1}^{\frac{M-1}{2}} x_{k-2mL}^2 + \sum_{m=0}^{\frac{M-3}{2}} x_{k-(2m+1)L}^2 \right) \tag{16}$$

$$\begin{aligned}\mu_{\text{odd}} = \sum_{k=(l-1)\beta+L+1}^{l\beta} \Bigg[&\left[\sum_{m=0}^{\frac{M-1}{2}} x_{k-2mL} + d_l \sum_{m=0}^{\frac{M-3}{2}} x_{k-(2m+1)L} \right] \\ &\times \left[\sum_{m=0}^{\frac{M-1}{2}} x_{k-(2m+1)L} + d_l \sum_{m=0}^{\frac{M-3}{2}} x_{k-(2m+2)L} \right] \Bigg] - \lambda_{\text{odd}}\end{aligned} \tag{17}$$

$$\begin{aligned}\nu_{\text{odd}} = \sum_{k=(l-1)\beta+L+1}^{l\beta} \Bigg[&\left(\sum_{m=0}^{\frac{M-1}{2}} x_{k-2mL} + d_l \sum_{m=0}^{\frac{M-3}{2}} x_{k-(2m+1)L} \right) \xi_{k-L} \\ &+ \left(\sum_{m=0}^{\frac{M-1}{2}} x_{k-(2m+1)L} + d_l \sum_{m=0}^{\frac{M-3}{2}} x_{k-(2m+2)L} \right) \xi_k + \xi_k \xi_{k-L} \Bigg]\end{aligned} \tag{18}$$

with $\{\lambda_{\text{even}}, \mu_{\text{even}}, \nu_{\text{even}}\}$ and $\{\lambda_{\text{odd}}, \mu_{\text{odd}}, \nu_{\text{odd}}\}$ denoting the sets of required signal, the intrasignal interference and the noise component when M is even and odd, respectively. Based on the value of y_l, the symbol is decoded according to (9). It can be observed that when L is small compared to β, the useful signal component in the GCDSK receiver is approximately $(M-1)$ times larger than that of the CDSK case. Although both the intrasignal interference and the noise component increase compared with the CDSK case, their effect can be compensated by the increase in signal component. Therefore, with appropriate values of M and L, GCDSK can be designed to outperform CDSK.

1) Gaussian-Approximated BERS: In our paper, we make use of the Chebyshev map of degree 2 to generate the chaotic signal. The map is given by

$$x_{k+1} = 2x_k^2 - 1 \tag{19}$$

and its correlation properties have been reported previously [6], [20]. Assuming that the chaotic signal $\{x_k\}$ is stationary, it is readily shown that for a given transmitted symbol d_l, the mean value of the correlator output equals

$$\mathrm{E}[y_l|d_l] = d_l(\beta - L)(M-1)P_s \tag{20}$$

where E[.] represents the expectation operator and

$$P_s = \mathrm{E}\left[x_k^2\right]. \tag{21}$$

If the conditional correlator output follows a Gaussian distribution, the approximate BER for the GCDSK system can then be derived analytically and is given by (22), as shown at the bottom of the page (see Appendix A for details), [see (23), shown at the bottom of the page], and the variables α, γ, P_c, and the functions V_1, V_2, V_3, C_1, C_2 are defined as in Appendix A.

IV. Results and Discussions

In this section, we present our findings on the bit error performance of the GCDSK system. We denote the average bit energy by E_b which can be readily shown equal to

$$E_b = \beta M P_s. \tag{24}$$

For various average-bit-energy-to-noise-psd (E_b/N_0) ratios, we simulate the GCDSK system and record the BERs. Also, we compute the approximate BERs using (22). We then compare our results with those derived from the CDSK and DCSK systems whenever appropriate.

A. Effect of Delay L

First, we investigate the effect of the delay L on the bit error performance. Fig. 3 plots the BER of the CDSK system together with that of the GCDSK system with $M = 4$ and 6.

$$\begin{aligned}\mathrm{BER}_{\mathrm{GCDSK}} &= \frac{1}{2}\mathrm{Prob}(y_l \le 0 \,|\, (d_l = +1)) + \frac{1}{2}\mathrm{Prob}(y_l > 0 \,|\, (d_l = -1)) \\ &= \begin{cases} \frac{1}{4}\mathrm{erfc}\left(\frac{(\beta-L)(M-1)P_s}{\sqrt{2\mathrm{var}[y_l|(d_l=+1)]}}\right) + \frac{1}{4}\mathrm{erfc}\left(\frac{(\beta-L)(M-1)P_s}{\sqrt{2\mathrm{var}[y_l\,|\,(d_l=-1)]}}\right), & \text{when } L = 1 \\ \frac{1}{2}\mathrm{erfc}\left(\frac{(\beta-L)(M-1)P_s}{\sqrt{2\mathrm{var}[y_l\,|\,(d_l=+1)]}}\right), & \text{when } 2 \le L < \beta \end{cases}\end{aligned} \tag{22}$$

$$\mathrm{var}[y_l\,|\,d_l] = \begin{cases} V_1(\beta,M)\mathrm{var}\left[x_k^2\right] + V_2(\beta,M){P_s}^2 + V_3(\beta,M)P_s\frac{N_0}{2} + (\beta-L)\frac{N_0^2}{4} \\ \quad +2d_lP_c[C_1(\beta,M) + C_2(\beta,M)], & \text{when } L = 1 \\ \alpha\left[V_1(\gamma+1,M)\mathrm{var}\left[x_k^2\right] + V_2(\gamma+1,M)P_s^2 + V_3(\gamma+1,M)P_s\frac{N_0}{2}\right] \\ \quad +(L-\alpha)\left[V_1(\gamma,M)\mathrm{var}\left[x_k^2\right] + V_2(\gamma,M)P_s^2 + V_3(\gamma,M)P_s\frac{N_0}{2}\right] \\ \quad +(\beta-L)\frac{N_0^2}{4}, & \text{when } 2 \le L < \beta \end{cases} \tag{23}$$

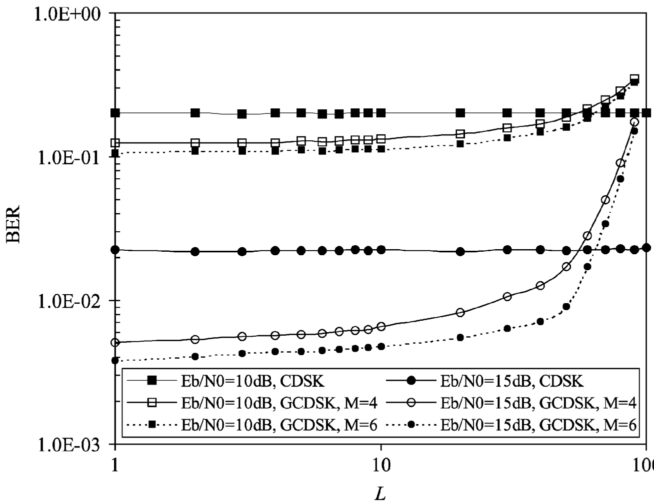

Fig. 3. Simulated BER versus delay L for CDSK and GCDSK systems. $\beta = 100$.

A spreading factor β of 100 is used. It is observed that the bit error performance for the GCDSK system degrades as the delay L increases. As stated in Section III-B, the correlator in the GDCSK receiver computes the sum of $(\beta - L)$ terms before deciding upon whether the received symbol is a "$+1$" or "-1." Hence, the correlator output becomes more unreliable when the number of terms reduces due to an increase in L, thereby increasing the BER. For the CDSK system, the number of the terms used in the correlator block is fixed at β and is independent of the delay L. Therefore, the bit error performance of the CDSK system is found to be unaffected by the delay L. Comparing the CDSK and GCDSK systems, it can be observed that for the same E_b/N_0, the GCDSK system outperforms the CDSK system with delay values up to 50.

In Fig. 4, the simulated BER is plotted against E_b/N_0 for the CDSK and GCDSK systems. The spreading factor is kept at 100. Again, it is shown that for a fixed E_b/N_0, the BER for the CDSK system is hardly affected by the delay L whereas the BER for the GCDSK system increases as L increases. As expected, the BER for both systems improves with increasing E_b/N_0.

B. Effect of the Number of Delay Blocks

Recall that in the GCDSK transmitter, the signal from the chaos generator is added to $M-1$ delayed chaotic signals (some are modulated by the symbol to be sent) before transmission. In Fig. 5, we plot the simulated BER against M. (Note that the CDSK system corresponds to the case where $M = 2$.) A spreading factor β of 100 is used. It is shown that for a fixed E_b/N_0 value, the BER reaches an optimal value at a certain value of M. Specifically, when M increases, the average bit energy and the detected signal component given by (24) and (20), respectively, increase initially. Although the intrasignal interference and the noise power also go up for a given E_b/N_0, there is a net improvement in the signal quality initially, thereby improving the BER. As the value of M is further increased beyond the optimal point, the percentage increase in the detected signal component is overshadowed by the degradation due to intrasignal interference and noise. Therefore, the BER starts to degrade for large values of M.

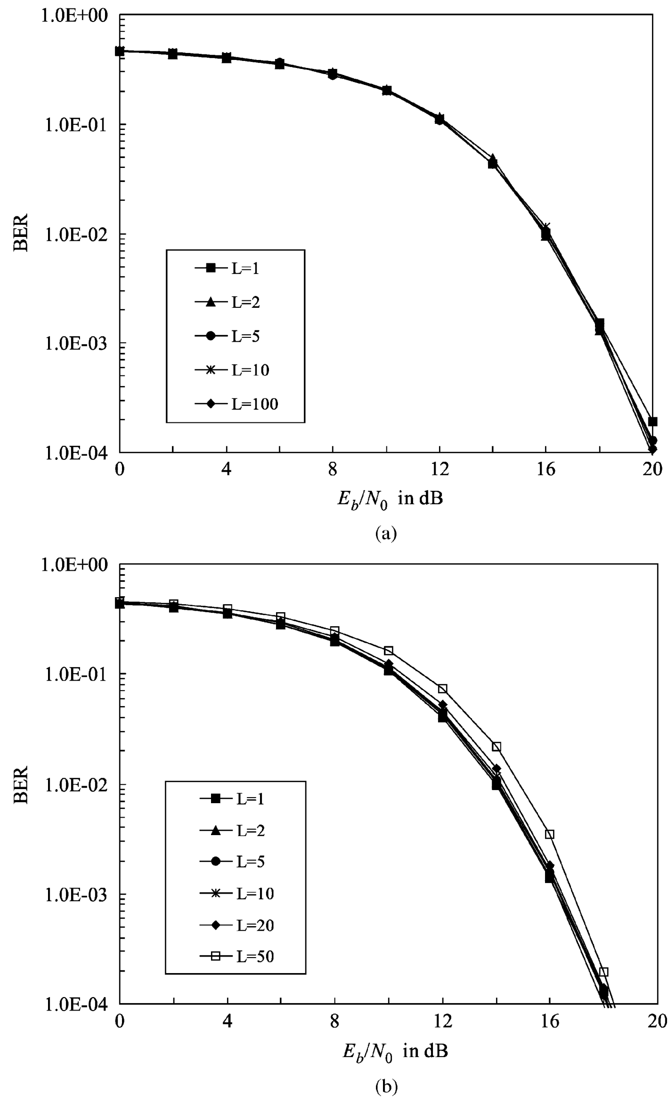

Fig. 4. Simulated BER versus $E_b/N_0 \cdot \beta = 100$. (a) CDSK system. (b) GCDSK system with $M = 6$.

C. Effect of Spreading Factor

Next, we study the effect of the spreading factor on the bit error performance. Fig. 6 plots the simulated BER versus the spreading factor. A delay value $L = 1$ is used. As in other noncoherent chaos-based communication systems, it is observed that the BER improves initially before an optimal point is reached [13], [18]. Apparently, the gain in the signal component is significant as the spreading factor first increases. Further increasing the spreading factor beyond the critical point degrades the performance because the increase in noise component become more prominent. It is also found that for different combinations of E_b/N_0 and M, the corresponding optimum values of β are different.

D. Comparison of the Simulated and Gaussian-Approximated BERS

Fig. 7 compares the simulated and Gaussian-approximated BERs for the CDSK and GCDSK systems. (See Appendix B for the derivation of the Gaussian-approximated BER for the CDSK system.) A spreading factor of 100 is used. In Fig. 7(a),

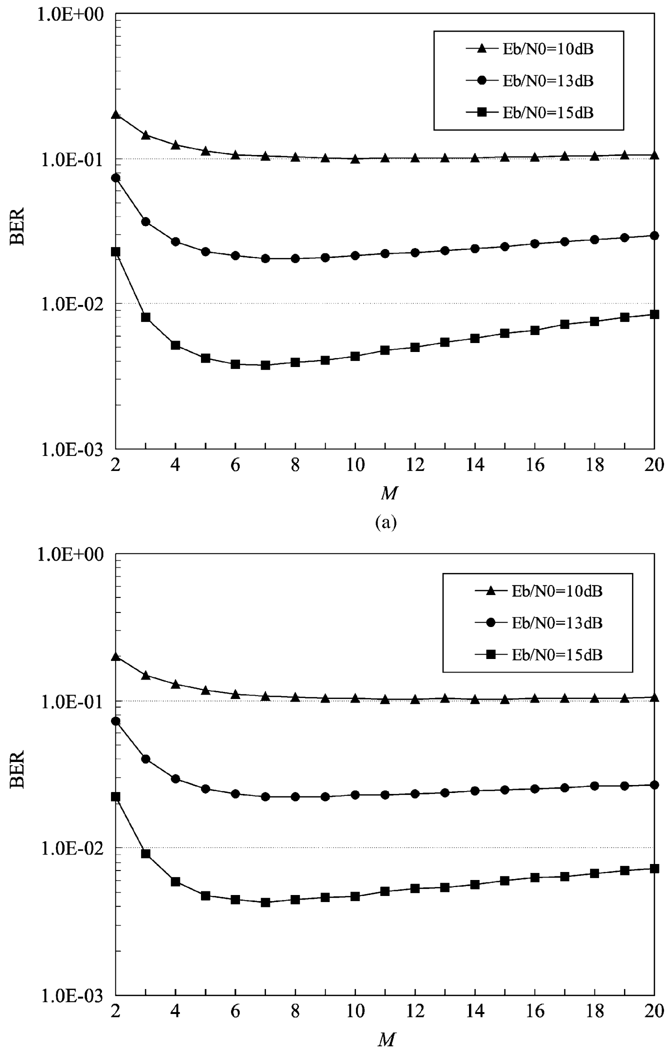

Fig. 5. Simulated BER versus M for the CDSK ($M = 2$) and GCDSK systems. $\beta = 100$. (a) $L = 1$. (b) $L = 5$.

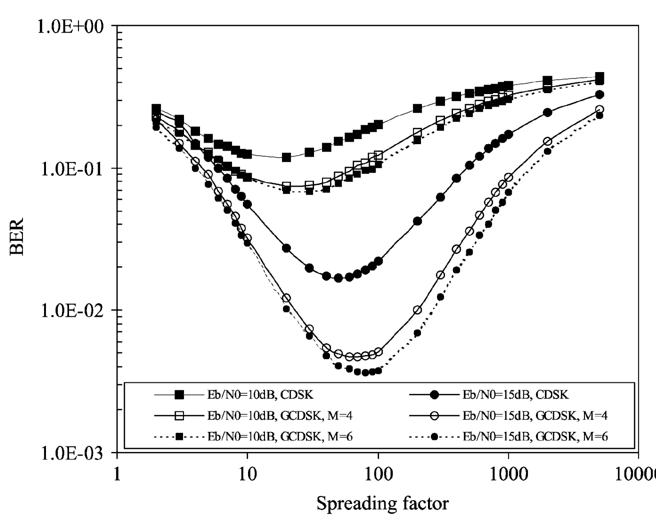

Fig. 6. Simulated BER versus spreading factor for the CDSK and GCDSK systems. $L = 1$.

it is observed that for the CDSK system, the simulated and Gaussian-approximated BERs are close when the delay L is

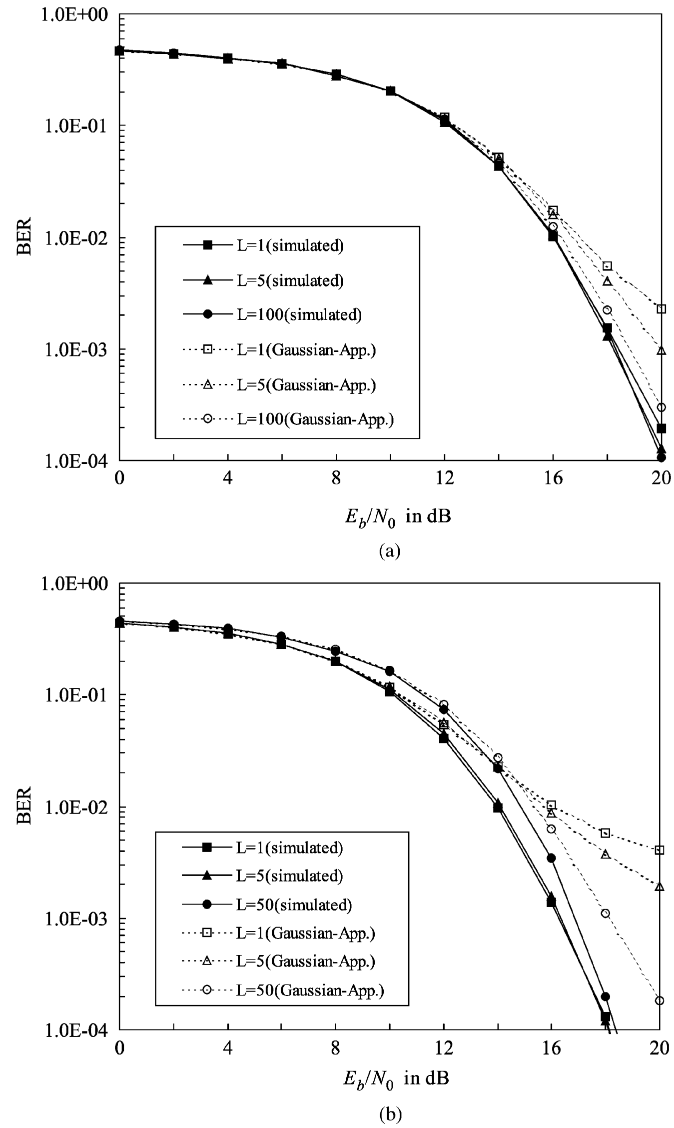

Fig. 7. Simulated and Gaussian-approximated BERs versus E_b/N_0. $\beta = 100$. Simulated results are plotted as solid lines and Gaussian-approximated results are plotted as dotted lines. (a) CDSK system. (b) GCDSK system with $M = 6$.

large, which is in good agreement with the results reported by Sushchik *et al.* [18]. For the GCDSK system with $M = 6$, the discrepancy between the simulated and Gaussian-approximated BERs is quite significant when E_b/N_0 is large. When we analyze the statistics of the correlator output from the simulation results, it is found that the conditional means and variances match with those derived in Appendix A. However, the distribution of the conditional correlator output does not follow a Gaussian distribution.

E. Comparison With DCSK System

Fig. 8 plots the simulated BERs of the GCDSK and DCSK systems. For the DCSK system, a spreading factor of $2\beta = 200$ is used. It can be observed that with a delay $L = 1$ and a spreading factor of $\beta = 100$, the GCDSK system can achieve similar BER performance as the DCSK system. In particular, when E_b/N_0 is lower than 16 dB, the GCDSK system slightly outperforms the DCSK one.

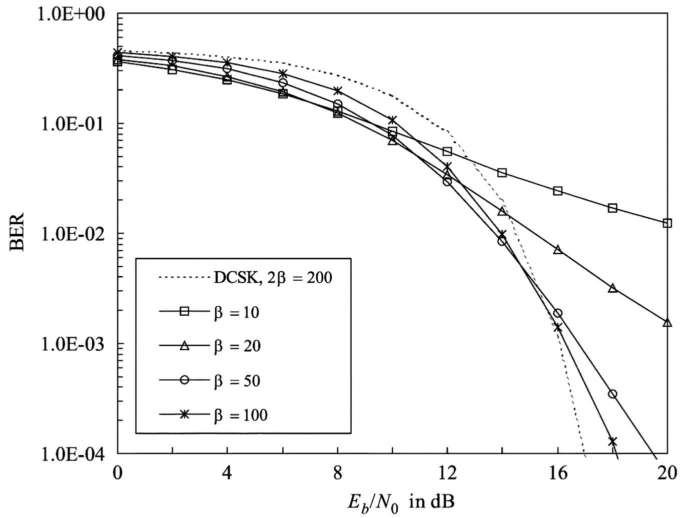

Fig. 8. Simulated BER versus E_b/N_0 for the GCDSK ($L = 1, M = 6$) and DCSK systems.

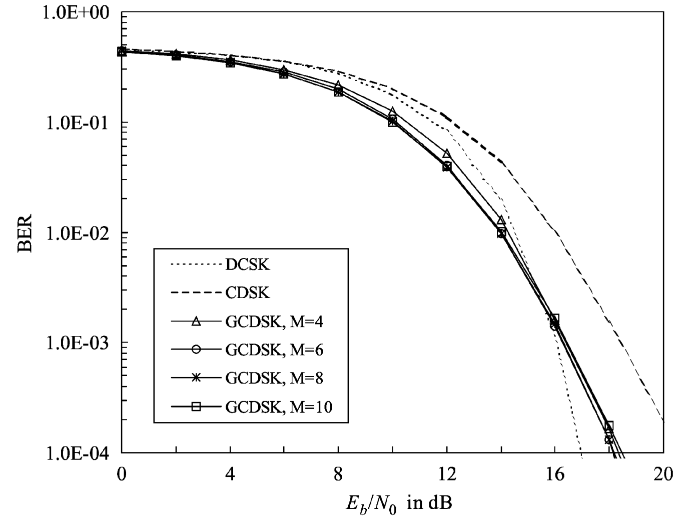

Fig. 9. Simulated BER versus E_b/N_0 for the CDSK, GCDSK, and DCSK systems. $\beta = 100$ for all systems. $L = 1$ for the CDSK and GCDSK systems.

In Fig. 9, the simulated BERs are plotted again for the CDSK, GCDSK, and DCSK systems. $\beta = 100$ is used for all systems and a delay of $L = 1$ is employed for the CDSK and GCDSK systems. It is found that the CDSK system gives the worst BER and is approximately 2 dB worse than the DCSK system. For the GCDSK system, the BERs are about the same for $M = 4, 6, 8,$ and 10. Its performance is similar to that of the DCSK system and is better for E_b/N_0 values below 16 dB.

V. Conclusion

In this paper, we develop and study in detail a GCDSK scheme for noncoherent chaos-based digital communications. We also compare the BER of the proposed system with two previously studied noncoherent chaos-based communication schemes, namely, CDSK scheme and DCSK scheme. Results show that the CDSK scheme gives the worst BER and is approximately 2 dB worse than the DCSK scheme. For the GCDSK scheme, the BERs are about the same as the DCSK scheme and are better for E_b/N_0 values below 16 dB. Further, we find that a simple Gaussian approximation is not sufficient to model the conditional correlator output at the receiver end. Hence, a more accurate model should be further investigated. In addition, as mentioned in Section III-B, part of the useful signal component is lost as a result of summing only $(\beta - L)$ terms in the receiver. The GCDSK system should thus be evaluated when a receiver that makes use of all useful signal component, i.e., β terms, is employed for demodulation.

Finally, it is also worthwhile to explore the possibility of extending the GCDSK scheme to allow multiple users within the system. One possible approach to differentiating the users is by assigning different delays to different users. At the receiving end, appropriate delays will be set to ensure that the data symbols of the desired user are decoded. Since different users are using different delays, the combination of the delay values would have a major effect on the system performance. Hence, various sets of delay values should be tested in optimizing the results.

Appendix A
Derivation of BERs for GCDSK System Based on Simple Gaussian Approximation

All symbols are defined as in Section III. Without loss of generality, we consider the probability of error for the lth symbol when all delay units at the transmitter side begin generating chaotic signals. Based on (12)–(18), it is readily shown that for a given transmitted symbol d_l, the mean value of y_l equals

$$\mathrm{E}[y_l \,|\, d_l] = d_l(\beta - L)(M-1)P_s \tag{25}$$

where E[.] denotes the expectation operator and

$$P_s = \mathrm{E}\left[x_k^2\right]. \tag{26}$$

In the evaluation of the variance of $y_l \,|\, d_l$, terms containing $d_l \mathrm{E}[x_k^2 x_{k+L} x_{k+2L}]$ appear. For the particular map $x_{k+1} = 2x_k^2 - 1$ that we are using

$$\mathrm{E}\left[x_k^2 x_{k+L} x_{k+2L}\right] \begin{cases} \neq 0, & \text{if } L = 1 \\ = 0, & \text{if } L > 1. \end{cases} \tag{27}$$

Thus, we derive the variance of $y_l|d_l$ under two different scenarios: $L = 1$ and $2 \leq L < \beta$. Note that when a different map is used, different nonzero terms containing d_l may appear.

When $L = 1$, the variance of $y_l|d_l$ can be shown equal to

$$\begin{aligned} \mathrm{var}[y_l \,|\, d_l] = {} & V_1(\beta, M)\mathrm{var}\left[x_k^2\right] + V_2(\beta, M){P_s}^2 \\ & + V_3(\beta, M)P_s\frac{N_0}{2} + (\beta - L)\frac{N_0^2}{4} \\ & + 2d_l P_c[C_1(\beta, M) + C_2(\beta, M)] \end{aligned} \tag{28}$$

where var[.] denotes the variance operator, and [see (29)–(34)at the bottom of the next page]. For the case when $2 \leq L < \beta$, we define

$$\gamma = \left\lfloor \frac{\beta - L}{L} \right\rfloor + 1 \tag{35}$$

$$\alpha = \beta - L - \left\lfloor \frac{\beta - L}{L} \right\rfloor L \tag{36}$$

where the function $\lfloor \varsigma \rfloor$ computes the integral part of ς. The variance of $y_l \,|\, d_l$ can be shown equal to

$$\begin{aligned}\mathrm{var}[y_l \,|\, d_l] = \alpha & \left[V_1(\gamma+1, M)\mathrm{var}\left[x_k^2\right] + V_2(\gamma+1, M)P_s^2 \right. \\ & \left. + V_3(\gamma+1, M)P_s\frac{N_0}{2}\right] \\ & + (L-\alpha)\left[V_1(\gamma, M)\mathrm{var}\left[x_k^2\right] \right. \\ & \left. + V_2(\gamma, M)P_s^2 + V_3(\gamma, M)P_s\frac{N_0}{2}\right] \\ & + (\beta - L)\frac{N_0^2}{4}. \end{aligned} \tag{37}$$

In this case, it can be observed that the variance of $y_l \,|\, d_l$ is independent of d_l.

If y_l follows a Gaussian distribution for a given transmitted symbol d_l, the approximate BER of the GDCSK system can be found as shown in (38) at the bottom of the page, where [see (39) at the bottom of the page] and $\mathrm{erfc}(\cdot)$ represents the complementary error function [1].

Appendix B
Derivation of Bit Error Rates for CDSK System Based on Simple Gaussian Approximation

All symbols are defined as in Section II. Without loss of generality, the probability of error for the lth symbol is considered.

$$P_c = \mathrm{E}\left[x_k^2 x_{k+1} x_{k+2}\right] \tag{29}$$

$$V_1(\beta, M) = \begin{cases} \sum_{u=1}^{M-1} u^2 + (\beta - M)(M-1)^2 + \sum_{u=1}^{M-2} u^2, & \text{when } \beta \geq M \\ \sum_{u=1}^{\beta-1} u^2 + (M-\beta)(\beta-1)^2 + \sum_{u=1}^{\beta-2} u^2, & \text{when } \beta < M \end{cases} \tag{30}$$

$$V_2(\beta, M) = \begin{cases} (\beta-1) + \sum_{u=0}^{M-2} 2(M-u-1)(2u+1)^2 + \sum_{u=1}^{M-1} (2u)^2(\beta-u-1), & \text{when } \beta \geq M \\ (\beta-1) + \sum_{u=0}^{\beta-2} 2(M-u-1)(2u+1)^2 + \sum_{u=1}^{\beta-2} (2u)^2(\beta-u-1) & \\ \quad +2(M-\beta+1)(M-\beta)(\beta-1)^2, & \text{when } \beta < M \end{cases} \tag{31}$$

$$V_3(\beta, M) = 2(2M\beta - 3M - 2\beta + 4) \tag{32}$$

$$C_1(\beta, M) = \begin{cases} \sum_{u=1}^{M-2}[(2u-1)^2 + (2u-1)(2u+1)] + (2M-3)(2M-4) & \\ \quad +(\beta-M)(2M-2)(2M-4), & \text{when } \beta \geq M > 2 \\ \sum_{u=1}^{\beta-1}(2u-1)^2 + \sum_{u=1}^{\beta-2}(2u-1)(2u+1) & \\ \quad +(2\beta-2)(2\beta-3) + 4(M-\beta-1)(\beta-1)^2, & \text{when } \beta < M \end{cases} \tag{33}$$

$$C_2(\beta, M) = \begin{cases} 8\beta - 20, & \text{when } \beta > M = 3 \\ \sum_{u=1}^{M-3}[u(2u+3) + (2u-1)(u+1)] + (M-2)(2M-2) & \\ \quad +(M-1)[(2M-3) + (2M-5)] + 2(\beta-M-1)(M-1)^2, & \text{when } \beta > M \geq 4 \\ 2M-5, & \text{when } 2 = \beta < M \\ 8M-20, & \text{when } 3 = \beta < M \\ \sum_{u=1}^{\beta-3}[u(2u+3) + (2u-1)(u+1)] + (\beta-2)(2\beta-2) & \\ \quad +(\beta-1)[(2\beta-3) + (2\beta-5)] + 2(M-\beta-1)(\beta-1)^2, & \text{when } 4 \leq \beta < M \\ \sum_{u=1}^{\beta-3}[u(2u+3) + (2u-1)(u+1)] + (\beta-2)(2\beta-3) & \\ \quad +(\beta-1)(2\beta-5), & \text{when } \beta = M \end{cases} \tag{34}$$

$$\begin{aligned}\mathrm{BER}_{\mathrm{GCDSK}} &= \frac{1}{2}\mathrm{Prob}(y_l \leq 0 \,|\, (d_l = +1)) + \frac{1}{2}\mathrm{Prob}(y_l > 0 \,|\, (d_l = -1)) \\ &= \begin{cases} \frac{1}{4}\mathrm{erfc}\left(\frac{(\beta-L)(M-1)P_s}{\sqrt{2\mathrm{var}[y_l \,|\, (d_l=+1)]}}\right) + \frac{1}{4}\mathrm{erfc}\left(\frac{(\beta-L)(M-1)P_s}{\sqrt{2\mathrm{var}[y_l \,|\, (d_l=-1)]}}\right), & \text{when } L = 1 \\ \frac{1}{2}\mathrm{erfc}\left(\frac{(\beta-L)(M-1)P_s}{\sqrt{2\mathrm{var}[y_l \,|\, (d_l=+1)]}}\right), & \text{when } 2 \leq L < \beta \end{cases}\end{aligned} \tag{38}$$

$$\mathrm{var}[y_l \,|\, d_l] = \begin{cases} V_1(\beta, M)\mathrm{var}\left[x_k^2\right] + V_2(\beta, M){P_s}^2 + V_3(\beta, M)P_s\frac{N_0}{2} + (\beta - L)\frac{N_0^2}{4} & \\ \quad +2d_l P_c[C_1(\beta, M) + C_2(\beta, M)], & \text{when } L = 1 \\ \alpha\left[V_1(\gamma+1, M)\mathrm{var}\left[x_k^2\right] + V_2(\gamma+1, M)P_s^2 + V_3(\gamma+1, M)P_s\frac{N_0}{2}\right] & \\ \quad +(L-\alpha)\left[V_1(\gamma, M)\mathrm{var}\left[x_k^2\right] + V_2(\gamma, M)P_s^2 + V_3(\gamma, M)P_s\frac{N_0}{2}\right] & \\ \quad +(\beta-L)\frac{N_0^2}{4}, & \text{when } 2 \leq L < \beta \end{cases} \tag{39}$$

$$\mathrm{E}[y_l \,|\, d_l] = d_l \beta P_s \tag{40}$$

$$\mathrm{var}[y_l \,|\, d_l] = \begin{cases} \beta\mathrm{var}\left[x_k^2\right] + (5\beta-2){P_s}^2 + \beta M P_s N_0 + \beta\frac{N_0^2}{4} + 8d_l(\beta-1)P_c, & \text{when } L = 1 \\ \theta W(\kappa+1) + (L-\theta)W(\kappa) + \beta M P_s N_0 + \beta\frac{N_0^2}{4}, & \text{when } 2 \leq L < \beta \\ \beta\mathrm{var}\left[x_k^2\right] + 3\beta P_s^2 + 2\beta P_s N_0 + \beta\frac{N_0^2}{4}, & \text{when } L \geq \beta \end{cases} \tag{41}$$

The derivation is similar to that of the GCDSK system and will not be shown here. In summary, we have (40) and (41), as shown at the bottom of the page, where

$$\kappa = \left\lfloor \frac{\beta}{L} \right\rfloor + 1 \tag{42}$$

$$\theta = \beta - \left\lfloor \frac{\beta}{L} \right\rfloor L \tag{43}$$

$$W(\psi) = (\psi - 1)\mathrm{var}\left[x_k^2\right] + (5\psi - 7){P_s}^2. \tag{44}$$

Note that for the case $L \geq \beta$, the variance of $y_l \,|\, d_l$ can be rewritten as

$$\mathrm{var}[y_l \,|\, d_l] = \beta \mathrm{var}\left[x_k^2\right] + \frac{3E_b^2}{4\beta} + E_b N_0 + \beta \frac{N_0^2}{4} \tag{45}$$

which is independent of d_l and can be shown equal to that obtained by Sushchik *et al.* [18]. The only difference is that the value of $\mathrm{var}[x_k^2]$ is different for different maps (symmetric tent map used by Sushchik *et al.* and Chebyshev map used here). The Gaussian-approximated BER can then be obtained similarly as in (38).

REFERENCES

[1] J. G. Proakis and M. Salehi, *Communications Systems Engineering*. Englewood Cliffs, NJ: Prentice-Hall, 1994.

[2] L. Kocarev, K. S. Halle, K. Eckert, L. O. Chua, and U. Parlitz, "Experimental demonstration of secure communications via chaotic synchronization," *Int. J. Bifurc. Chaos*, vol. 2, no. 3, pp. 709–713, Mar. 1992.

[3] H. Dedieu, M. P. Kennedy, and M. Hasler, "Chaos shift keying: Modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuit," *IEEE Trans. Circuits Syst. II, Analog Digit. Signal Process.*, vol. 40, no. 11, pp. 634–642, Nov. 1993.

[4] M. Itoh and H. Murakami, "New communication systems via chaotic synchronizations and modulation," *IEICE Trans. Fundamentals*, vol. E78-A(3), pp. 285–290, 1995.

[5] G. Kolumbán, M. P. Kennedy, and L. O. Chua, "The role of synchronization in digital communications using chaos—Part II: Chaotic modulation and chaotic synchronization," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 45, no. 11, pp. 1129–1140, Nov. 1998.

[6] F. C. M. Lau and C. K. Tse, *Chaos-Based Digital Communication Systems*. Heidelberg, Germany: Springer-Verlag, 2003.

[7] G. Kolumbán, G. K. Vizvari, W. Schwarz, and A. Abel, "Differential chaos shift keying: A robust coding for chaos communication," in *Proc. Int. Workshop on Nonlinear Dynamics of Electron. Syst.*, Seville, Spain, 1996, pp. 87–92.

[8] G. Kolumbán and M. P. Kennedy, "The role of synchronization in digital communications using chaos—Part III: Performance bounds for correlation receivers," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 47, no. 12, pp. 1673–1683, Dec. 2000.

[9] G. Kolumbán, M. P. Kennedy, Z. Jákó, and G. Kis, "Chaotic communications with correlator receiver: Theory and performance limit," *Proc. IEEE*, vol. 90, no. 5, pp. 711–732, May 2002.

[10] M. Hasler and T. Schimming, "Chaos communication over noisy channels," *Int. J. Bifurc. Chaos*, vol. 10, pp. 719–735, 2000.

[11] F. C. M. Lau and C. K. Tse, "On optimal detection of noncoherent chaos-shift-keying signals in a noisy environment," *Int. J. Bifurc. Chaos*, vol. 13, no. 6, pp. 1587–1597, 2003.

[12] ——, "Approximate-optimal detection for chaos communication systems," *Int. J. Bifurc. Chaos*, vol. 13, no. 5, pp. 1329–1335, 2003.

[13] C. K. Tse, K. Y. Cheong, F. C. M. Lau, and S. F. Hau, "Return-map-based approaches for noncoherent detection in chaotic digital communications," *IEEE Circuits Syst. I, Fundam. Theory Appl.*, vol. 49, no. 10, pp. 1495–1499, Oct. 2002.

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

[15] M. P. Kennedy and G. Kolumbán, "Digital communication using chaos," in *Controlling Chaos and Bifurcation in Engineering Systems*, G. Chen, Ed. Boca Raton, FL: CRC, 2000, pp. 477–500.

[16] 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.

[17] 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, Jun. 2003.

[18] 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.

[19] W. M. Tam, F. C. M. Lau, and C. K. Tse, "Analysis of bit error rates for multiple access CSK and DCSK communication systems," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 50, no. 5, pp. 702–707, May 2003.

[20] T. Geisel and V. Fairen, "Statistical properties of chaos in Chebyshev maps," *Phys. Lett. A*, vol. 105A, no. 6, pp. 263–266, 1984.

Wai M. Tam received the B.Sc. degree in electronics and information systems from Jinan University, China, and the M.Phil. and Ph.D. degrees in electronic and information engineering from The Hong Kong Polytechnic University, Hong Kong.

She is currently a Postdoctoral Fellow with the Department of Electronic and Information Engineering, The Hong Kong Polytechnic University. Her research interests include power control in CDMA mobile cellular systems, third-generation mobile systems, and chaos-based digital communications.

In 2003, Dr. Tam was awarded the Li Po Chun Charitable Trust Fund Scholarship and the Chung Hwa Travel Services Scholarship, and in 2004 The Hong Kong Polytechnic University Postdoctoral Fellowship.

Francis C. M. Lau (M'93–SM'03) received the B.Eng. (Hons.) degree (with first class honors) in electrical and electronic engineering and the Ph.D. degree from King's College London, University of London, U.K., in 1989 and 1993, respectively.

He is an Associate Professor and the Leader of the Communication Engineering Section, Department of Electronic and Information Engineering, The Hong Kong Polytechnic University, Hong Kong. He is the coauthor of *Chaos-Based Digital Communication Systems* (Springer-Verlag, 2003). His main research interests include power control and capacity analysis in mobile communication systems, and chaos-based digital communications.

Chi K. Tse (M'90–SM'97–F'06) received the B.Eng. (Hons.) degree (with first class honors) in electrical engineering and the Ph.D. degree from the University of Melbourne, Australia, in 1987 and 1991, respectively.

He is presently a Professor with The Hong Kong Polytechnic University, Hong Kong. His research interests include chaotic dynamics, power electronics, and chaos-based communications. He is the author of *Linear Circuit Analysis* (Addison-Wesley, 1998) and *Complex Behavior of Switching Power Converters* (CRC, 2003), coauthor of *Chaos-Based Digital Communication Systems* (Springer-Verlag, 2003), and coholder of a U.S. patent.

Prof. Tse served as an Associate Editor for the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—I: FUNDAMENTAL THEORY AND APPLICATIONS from 1999 to 2001. Since 1999, he has been an Associate Editor for the IEEE TRANSACTIONS ON POWER ELECTRONICS. He also currently serves as an Associate Editor for the *International Journal of Systems Science*. In 1987, he was awarded the L.R. East Prize by the Institution of Engineers, Australia, and in 2001, the IEEE TRANSACTIONS ON POWER ELECTRONICS Prize Paper Award. While with the university, he received the President's Award for Achievement in Research twice, the Faculty's Best Researcher Award, and a few other teaching awards. Since 2002, he has been appointed as Guest Professor by the Southwest China Normal University, Chongqing, China. In 2006, he was elected a Fellow of the IEEE for contributions to power electronics circuits and applications.