Permutation-Based DCSK and Multiple-Access DCSK Systems

Francis C. M. Lau, *Senior Member, IEEE*, Kai Y. Cheong, and Chi K. Tse, *Senior Member, IEEE*

***Abstract*—This paper presents a method for enhancing the differential chaos-shift-keying (DCSK) and multiple access DCSK systems. By introducing a permutation transformation which destroys the similarity between the reference and data samples in a DCSK system, the bit rate can be made undetectable from the frequency spectrum, thereby enhancing the data security. Using different transformations for different users, the interference between users in a multiple-access system can be minimized, and each symbol is ensured to be sent within one bit duration for all users. Furthermore, the implementation requires only slight modification to the original DCSK system.**

***Index Terms*—Chaos communication, differential chaos-shift-keying, multiple access.**

I. Introduction

EVER since Pecaro and Carroll demonstrated experimentally that two coupled chaotic systems can be synchronized [1], researchers have shown increasing interest in the application of chaos to communications. By using a chaotic carrier to spread the digital signal over a wide bandwidth, the resulting system inherits the benefits of spread-spectrum communications such as mitigation of multipath fading and low probability of detection. A number of chaos-based communication schemes have been proposed and studied in recent years, including chaos masking [2], [3], chaotic switching or chaos shift keying (CSK) [4] and [5], differential CSK (DCSK) [6] and frequency-modulated DCSK (FM-DCSK) [7]. Among the digital communication techniques proposed, CSK and DCSK are the most widely studied [8]–[12]. In DCSK, each bit duration is divided into two equal slots. In the first slot, a reference chaotic signal is sent. Dependent upon the symbol being sent, the reference signal is either repeated or multiplied by the factor "-1" and transmitted in the second slot. The advantage of DCSK over CSK is that the threshold level at the receiver is always set at zero and is independent of the noise level. However, as will be shown later, the bit frequency can be easily determined from the transmitted signal, jeopardizing the security of the system.

To make efficient use of the frequency spectrum occupied by the chaotic signals, several multiple-access schemes have been proposed recently for chaos-based communication systems. Approaches have been developed for chaotic functions to generate spreading codes which are applied to conventional code-division multiple-access (CDMA) systems [13]–[15]. Also, the use of chaotic frequency modulation (CFM) has been extended to multi-user communications [16]. In the multi-user CFM scheme, the base station transmits a reference signal with chaotically varying frequency. All users are first required to synchronize their chaotic oscillators to the reference signal. Then, every transmitter applies its own unique transformation to the synchronized chaotic waveform to generate its information-carrying CFM signal. The band in which the mobile units are transmitting the CFM signals is separated from the band used for "synchronization" such that the reference CFM signal is free from interference. In Tam *et al.* [17], a multiple-access technique based on CSK has been proposed and the analytical bit-error rate (BER) is derived and compared with simulation results.

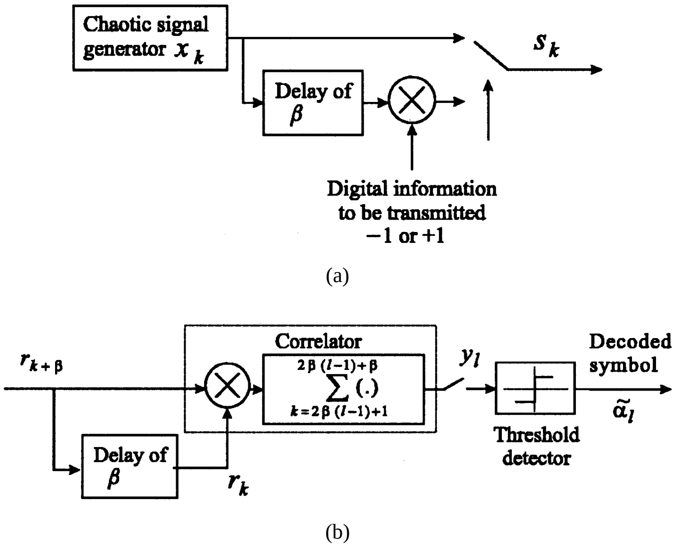
Multiple access based on DCSK was first introduced by Kolumbán *et al.* [18], [19]. Afterwards, Jako *et al.* [20] studied the multiple-access capability of FM-DCSK. In both cases, two chaotic basis functions have been used to transmit two streams of data at the same time in the same frequency band. The bit period is first divided into four time slots. For the first signal, the reference sample is divided into two parts which are sent in the first and third time slots. Similarly, the data sample is also divided into two parts which are sent in the second and fourth time slots. To achieve low interference between the transmitted signals, the order of transmission is changed for the second signal. The reference sample is sent in the first two slots while the data sample is transmitted in the third and fourth slots. If the two chaotic basis functions are uncorrelated, the two signals will not affect each other when appropriate demodulation techniques are used. When the number of users increases, however, the number of time slots created in each bit duration would also increase, implying that switching between the reference and data samples will be performed more frequently within the same bit period. This will impose more stringent requirements on the switching circuits in both the transmitter and the receiver. Another multiple-access technique for use with DCSK (MA-DCSK) is proposed and analyzed by Lau *et al.* [21]. The proposed scheme gives equal average data rates for all users. As in a single-user DCSK system, each bit duration is divided into two time slots for all users. Here, the requirements on the switching circuits in the transmitter and the receiver will be similar compared with the single-user system. To minimize the correlation between signals from different users, the frame periods and the arrangements of the reference and sample waveforms of all users are different, and each user

Manuscript received March 11, 2002; revised June 23, 2002. This work was supported in part by The Hong Kong Polytechnic University and in part by the Hong Kong Research Grants Council under Grant PolyU5137/02E. 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: encmlau@polyu.edu.hk; 01900720r@polyu.edu.hk; encktse@polyu.edu.hk).

Digital Object Identifier 10.1109/TCSI.2003.812616

1057-7122/03$17.00 © 2003 IEEE


Chaotic signal generator x_k
Delay of β
s_k
Digital information to be transmitted −1 or +1
Correlator
$r_{k+\beta}$
$\sum_{k=2\beta(l-1)+1}^{2\beta(l-1)+\beta}(.)$
y_l
Decoded symbol
$\tilde{\alpha}_l$
Threshold detector
Delay of β
r_k

(a)

(b)

Fig. 1. Block diagram of a noncoherent DCSK system. (a) Modulator. (b) Demodulator.

has to receive half of the frame before demodulation can begin. As a consequence, different users will experience different demodulation delays although the average bit rates of all users are the same. Also, the MA-DCSK system is substantially different from that of the single-user system.

In this paper, a permutation approach for enhancing the DCSK scheme is proposed. In Section II, the operation of a conventional DCSK system is briefly reviewed, and in Section III, the proposed DCSK scheme is described. The frequency spectra of both systems will be compared. In Section IV, the proposed DCSK scheme is extended to a multiple-access environment and the system operation is explained in detail. The analytical and simulation results are also presented and compared with a previously proposed MA-DCSK scheme.

II. DCSK

A. System Overview

DCSK was first proposed by Kolumbán *et al.* [6]. By using a chaotic carrier to spread the digital signal over a wide bandwidth, the resulting system shares some of the advantages of spread-spectrum communications such as mitigation of multipath fading and low probability of detection. In DCSK, each bit duration is first divided into two equal time slots and every transmitted symbol is represented by two sets of chaotic signal samples sent in the two slots. The first sample set serves as the reference (reference sample) while the second one carries the data (data sample). If a “+1” is to be transmitted, the data sample will be identical to the reference sample, and if a “−1” is to be transmitted, an inverted version of the reference sample will be used as the data sample. Fig. 1 shows the block diagrams of the modulator and demodulator of a noncoherent DCSK system. Assume that the system is discrete. Let 2β be the spreading factor, defined as the number of chaotic samples sent for each binary symbol, where β is an integer. Denote the lth transmitted symbol by $\alpha_l \in \{-1, +1\}$. During the lth bit duration, i.e., for time $k = 2\beta(l-1)+1, 2\beta(l-1)+2, \ldots, 2\beta l$, the output of the transmitter, s_k, is

$$s_k = \begin{cases} x_k, & \text{for } k = 2\beta(l-1)+1 \\ & \quad 2\beta(l-1)+2, \ldots, 2\beta(l-1)+\beta, \\ \alpha_l x_{k-\beta}, & \text{for } k = 2\beta(l-1)+\beta+1, \\ & \quad 2\beta(l-1)+\beta+2, \ldots, 2\beta l. \end{cases} \tag{1}$$

The transmitted signal, after passing through the channel, which is assumed to be additive white Gaussian, arrives at the receiver. At time k, the received signal r_k, is given by

$$r_k = s_k + \xi_k \tag{2}$$

where ξ_k denotes the additive white Gaussian noise with zero mean and variance (power spectral density) $N_0/2$. At the receiving end, the reference sample and the corresponding data sample are correlated. The output of the correlator at the end of the lth symbol duration is given by

$$y_l = \sum_{k=2\beta(l-1)+1}^{2\beta(l-1)+\beta} r_k r_{k+\beta}. \tag{3}$$

Depending on whether the output y_l is larger or smaller than the threshold zero, a “+1” or “−1” is decoded.

To simplify the notations, we define

$$\boldsymbol{x}_l = \left(x_{2\beta(l-1)+1} \;\; x_{2\beta(l-1)+2} \;\; \cdots \;\; x_{2\beta(l-1)+\beta}\right) \tag{4}$$

$$\Psi_m = \left(\xi_{\beta m+1} \;\; \xi_{\beta m+2} \;\; \cdots \;\; \xi_{\beta m+\beta}\right) \tag{5}$$

$$\boldsymbol{s}_l = \big(s_{2\beta(l-1)+1} \;\; s_{2\beta(l-1)+2} \;\; \cdots \;\; s_{2\beta(l-1)+\beta} \;\; s_{2\beta(l-1)+\beta+1} \;\; \cdots \;\; s_{2\beta l}\big) \tag{6}$$

$$\boldsymbol{r}_l = \big(r_{2\beta(l-1)+1} \;\; r_{2\beta(l-1)+2} \;\; \cdots \;\; r_{2\beta(l-1)+\beta} \;\; r_{2\beta(l-1)+\beta+1} \;\; \cdots \;\; r_{2\beta l}\big). \tag{7}$$

Thus, during the lth symbol duration, the transmitted signal block, $\boldsymbol{s}_l$, can be denoted by

$$\boldsymbol{s}_l = (\boldsymbol{x}_l \;\; \alpha_l \boldsymbol{x}_l) \tag{8}$$

whereas the received signal block, $\boldsymbol{r}_l$, is now represented by

$$\boldsymbol{r}_l = (\boldsymbol{x}_l + \Psi_{2l-2} \;\; \alpha_l \boldsymbol{x}_l + \Psi_{2l-1}). \tag{9}$$

Further, the correlator output is simplified to

$$y_l = (\boldsymbol{x}_l + \Psi_{2l-2})(\alpha_l \boldsymbol{x}_l + \Psi_{2l-1})^T \tag{10}$$

where superscript T denotes matrix transposition.

B. Frequency Spectra

In this section, we analyze the frequency spectrum of a 10-bit DCSK signal sample. Fig. 2 plots the magnitude of the spectrum. It can be seen that the spectrum is white and no useful information can be retrieved. Next, we square the DCSK signal sample and plot the magnitude spectrum again. From Fig. 3, it can be clearly observed that the spectral value goes to zero at odd multiple frequencies of the bit rate. This observation can be explained as follows. When the DCSK signal sample is squared, the resultant signals in the information-bearing slots become identical to their corresponding reference slots. Thus, no frequency component at odd multiples of the bit rate (i.e., any multiples of slot rate) exists because any contributions from the information-bearing slots will be cancelled exactly by those from

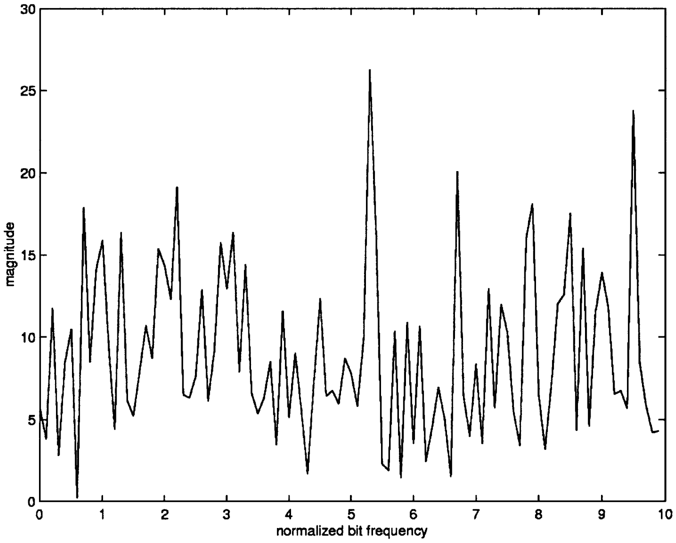


Fig. 2. Magnitude of frequency components versus normalized bit frequency for a conventional DCSK signal sample.

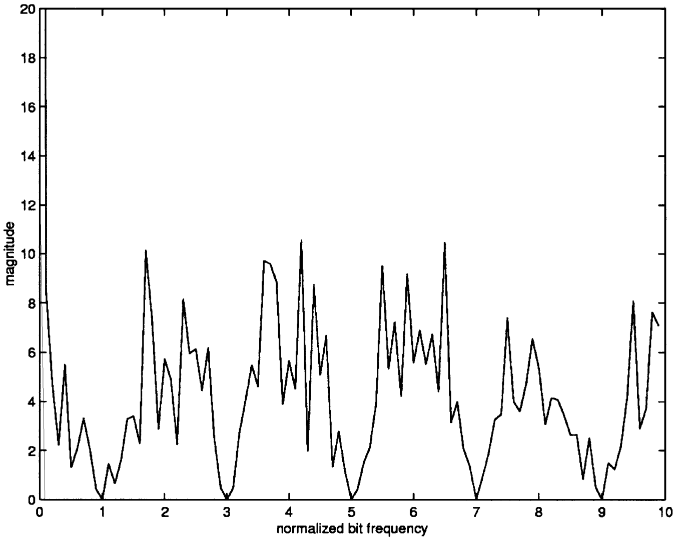


Fig. 3. Magnitude of frequency components versus normalized bit frequency for the square of a conventional DCSK signal sample.

the reference slots at such frequencies. This may not be very desirable because anyone, intended or unintended, can retrieve the bit rate of the DCSK system easily.

III. Permutation-Based DCSK System

A. System Description

Fig. 4 depicts the block diagram of the proposed permutation-based DCSK (P-DCSK) system. In this scheme, each signal block undergoes a transformation F before transmission, and the transmitted block, denoted by $\boldsymbol{u}_l$, equals

$$\boldsymbol{u}_l = F(\boldsymbol{s}_l). \tag{11}$$

At the receiver, we write the lth received signal block as $\boldsymbol{v}_l = \boldsymbol{u}_l + (\Psi_{2l-2} \;\; \Psi_{2l-1})$. The incoming block will first undergo an inverse transformation $G = F^{-1}$ to retrieve an output block $\boldsymbol{r}_l$, i.e.,

$$\boldsymbol{r}_l = G(\boldsymbol{v}_l). \tag{12}$$

The output block $\boldsymbol{r}_l$ is then passed to a conventional DCSK demodulator for decoding. Comparing with the conventional DCSK system, additional transformation and inverse transformation are needed in the transmitter and receiver, respectively. The objective of the additional transformations is to eliminate the bit rate information in the frequency spectrum.

In this paper, we propose the use of permutation in the transformation process. Specifically, the transformation and inverse transformation are given, respectively, by

$$F(\boldsymbol{s}_l) = \boldsymbol{s}_l \boldsymbol{P}_{2\beta} \tag{13}$$

and

$$G(\boldsymbol{v}_l) = F^{-1}(\boldsymbol{v}_l) = \boldsymbol{v}_l(\boldsymbol{P}_{2\beta})^{-1} = \boldsymbol{v}_l(\boldsymbol{P}_{2\beta})^T \tag{14}$$

where $\boldsymbol{P}_{2\beta}$ is a $2\beta \times 2\beta$ permutation matrix [22] in which the elements are either "0" or "1" and there is exactly one "1" in each row and in each column.

B. Frequency Spectra

The frequency spectra of the P-DCSK signal sample and the square of the sample are plotted in Figs. 5 and 6, respectively. It can be seen that in both cases the spectrum is white and no bit rate information can be retrieved. Hence, the data security is enhanced. For the intended receiver with complete knowledge of the permutation matrix, nonetheless, bit synchronization can still be easily accomplished for demodulation purposes.

IV. Permutation-Based MA-DCSK System

In this section, we apply the aforementioned P-DCSK scheme to a multiple-access environment.

A. System Description

Fig. 7 depicts the block diagram of a permutation-based MA-DCSK (PMA-DCSK) system. Denote the lth transmitted symbol of user i by $\alpha_l^{(i)}$. The corresponding signal block will be given by

$$\begin{aligned}\boldsymbol{s}_l^{(i)} &= \Big(s_{2\beta(l-1)+1}^{(i)} \;\; s_{2\beta(l-1)+2}^{(i)} \;\; \cdots \;\; s_{2\beta(l-1)+\beta}^{(i)} \\ &\qquad s_{2\beta(l-1)+\beta+1}^{(i)} \;\; \cdots \;\; s_{2\beta l}^{(i)}\Big) \\ &= \Big(\boldsymbol{x}_l^{(i)} \;\; \alpha_l^{(i)}\boldsymbol{x}_l^{(i)}\Big)\end{aligned} \tag{15}$$

where

$$\boldsymbol{x}_l^{(i)} = \Big(x_{2\beta(l-1)+1}^{(i)} \;\; x_{2\beta(l-1)+2}^{(i)} \;\; \cdots \;\; x_{2\beta(l-1)+\beta}^{(i)}\Big) \tag{16}$$

and $\{x_k^{(i)}\}$ represents the chaotic sequence generated by the ith chaos generator. In the PMA-DCSK scheme, each signal block of the ith user undergoes a permutation-transformation F_i before transmission, and the transmitted block, denoted by $\boldsymbol{u}_l^{(i)}$, equals

$$\begin{aligned}\boldsymbol{u}_l^{(i)} &= \Big(u_{2\beta(l-1)+1}^{(i)} \;\; u_{2\beta(l-1)+2}^{(i)} \;\; \cdots \;\; u_{2\beta(l-1)+\beta}^{(i)} \\ &\qquad u_{2\beta(l-1)+\beta+1}^{(i)} \;\; \cdots \;\; u_{2\beta l}^{(i)}\Big) \\ &= F_i\left(\boldsymbol{s}_l^{(i)}\right) \\ &= \boldsymbol{s}_l^{(i)}\boldsymbol{P}_{2\beta}^{(i)}\end{aligned} \tag{17}$$

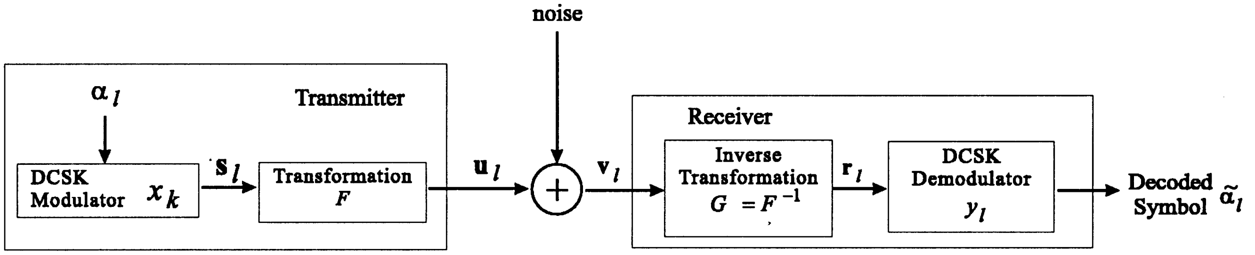


Fig. 4. Proposed P-DCSK communication system.

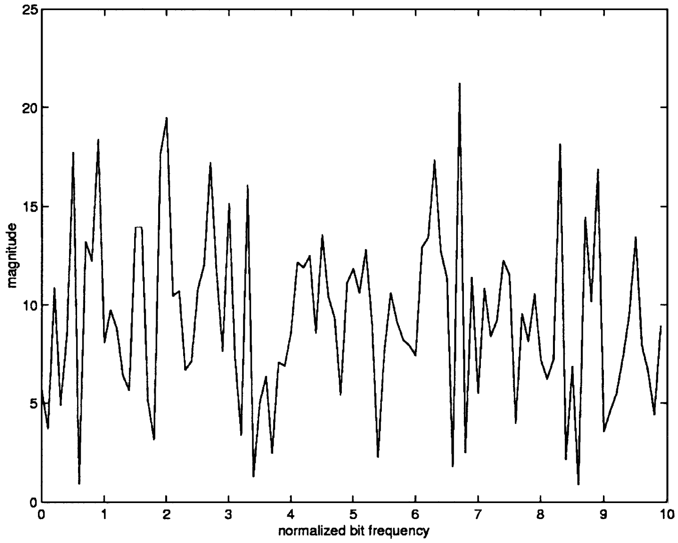


Fig. 5. Magnitude of frequency components versus normalized bit frequency for a P-DCSK signal sample.

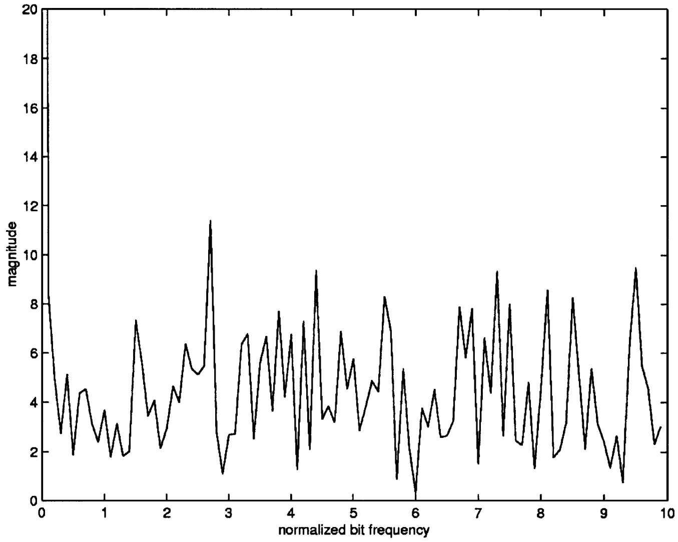


Fig. 6. Magnitude of frequency components versus normalized bit frequency for the square of a P-DCSK signal sample.

where $\boldsymbol{P}_{2\beta}^{(i)}$ is a $2\beta \times 2\beta$ permutation matrix used by user i. The overall transmitted signal block of the whole system during the lth bit duration, denoted by $\boldsymbol{u}_l$, is derived by summing the signals of all users, i.e.,

$$\boldsymbol{u}_l = \sum_{i=1}^{N} \boldsymbol{u}_l^{(i)} = \sum_{i=1}^{N} \boldsymbol{s}_l^{(i)} \boldsymbol{P}_{2\beta}^{(i)}. \tag{18}$$

At the jth receiver, denote the lth received signal block by $\boldsymbol{v}_l = \boldsymbol{u}_l + (\Psi_{2l-2} \;\; \Psi_{2l-1})$. The incoming block will first undergo an inverse transformation $G_j = F_j^{-1}$ to retrieve an output block $\boldsymbol{r}_l^{(j)}$, i.e.,

$$\begin{aligned}
\boldsymbol{r}_l^{(j)} &= G_j(\boldsymbol{v}_l) \\
&= (\boldsymbol{u}_l + (\Psi_{2l-2} \;\; \Psi_{2l-1})) \left(\boldsymbol{P}_{2\beta}^{(j)}\right)^T \\
&= \boldsymbol{u}_l \left(\boldsymbol{P}_{2\beta}^{(j)}\right)^T + (\Psi_{2l-2} \;\; \Psi_{2l-1}) \left(\boldsymbol{P}_{2\beta}^{(j)}\right)^T \\
&= \sum_{i=1}^{N} \boldsymbol{s}_l^{(i)} \boldsymbol{P}_{2\beta}^{(i)} \left(\boldsymbol{P}_{2\beta}^{(j)}\right)^T + (\Psi_{2l-2} \;\; \Psi_{2l-1}) \left(\boldsymbol{P}_{2\beta}^{(j)}\right)^T \\
&= \boldsymbol{s}_l^{(j)} + \sum_{\substack{i=1 \\ i\neq j}}^{N} \boldsymbol{s}_l^{(i)} \boldsymbol{P}_{2\beta}^{(i)} \left(\boldsymbol{P}_{2\beta}^{(j)}\right)^T + (\Psi_{2l-2} \;\; \Psi_{2l-1}) \left(\boldsymbol{P}_{2\beta}^{(j)}\right)^T \\
&= \underbrace{\boldsymbol{s}_l^{(j)}}_{\text{required DCSK signal of user } j} + \underbrace{\sum_{\substack{i=1 \\ i\neq j}}^{N} \boldsymbol{s}_l^{(i)} \boldsymbol{P}_{2\beta}^{(i,j)}}_{\text{interference from other users}} \\
&\quad + \underbrace{(\Psi_{2l-2} \;\; \Psi_{2l-1}) \left(\boldsymbol{P}_{2\beta}^{(j)}\right)^T}_{\text{noise}}
\end{aligned} \tag{19}$$

where

$$\boldsymbol{P}_{2\beta}^{(i,j)} = \boldsymbol{P}_{2\beta}^{(i)} \left(\boldsymbol{P}_{2\beta}^{(j)}\right)^T. \tag{20}$$

The matrix $\boldsymbol{P}_{2\beta}^{(i,j)}$, being the product of two permutation matrices, is also a permutation matrix. The output block $\boldsymbol{r}_l^{(j)}$ is then passed to a conventional DCSK demodulator for decoding.

To ensure that the inter-user interference is kept to a low level, it is necessary and sufficient that the $(\lambda + \beta)$th $(\lambda = 1, 2, \ldots, \beta)$ element in $\boldsymbol{s}_l^{(i)} \boldsymbol{P}_{2\beta}^{(i,j)}$ $(i \neq j)$ should not equal to the λth element or its negation. In other words, in $\boldsymbol{P}_{2\beta}^{(i,j)}$, the nonzero elements in the λth $(\lambda = 1, 2, \ldots, \beta)$ and $(\lambda + \beta)$th rows should not differ by β columns. Denote the element in the ath row and bth column in the matrix $\boldsymbol{P}_{2\beta}^{(i,j)}$ by $p_{a,b}^{(i,j)}$. If the nonzero elements in the λth and $(\lambda + \beta)$th rows are $p_{\lambda,\mu}^{(i,j)}$ and $p_{\lambda+\beta,\nu}^{(i,j)}$, respectively, then $|\mu - \nu| \neq \beta$. There are many ways to choose the permutation matrices such that the aforementioned condition is satisfied. One simple example, based on a random

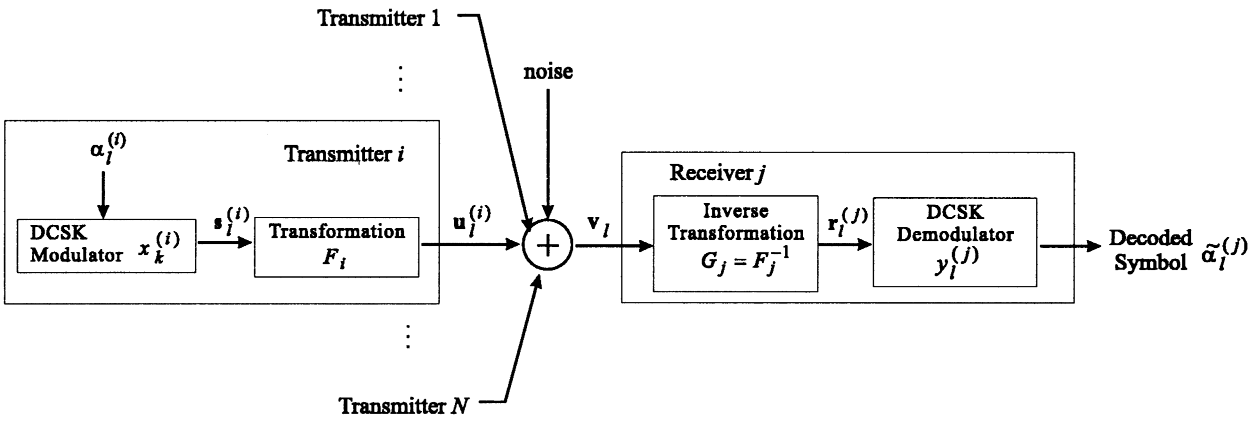


Fig. 7. Proposed MA-DCSK communication system.

permutation matrix and a "shifting" matrix, is described in Appendix A. We assume that all users use the cubic map

$$x_{k+1} = g(x_k) = 4x_k^3 - 3x_k \tag{21}$$

to generate the chaotic sequences, and each uses a different initial condition. Based on the permutation matrices constructed in Appendix A, the analytical BER can be found as (see Appendix B)

$$\mathrm{BER}^{(j)} = \frac{1}{2}\,\mathrm{erfc}\left(\left[\frac{2\Omega}{\beta} + \frac{2(N^2-1)}{\beta} + 4N\left(\frac{E_b}{N_0}\right)^{-1} + 2\beta\left(\frac{E_b}{N_0}\right)^{-2}\right]^{-(1/2)}\right) \tag{22}$$

where the complementary error function, $\mathrm{erfc}(.)$, is defined as

$$\mathrm{erfc}(\psi) \equiv \frac{2}{\sqrt{\pi}}\int_{\psi}^{\infty} e^{-\lambda^2}\,d\lambda. \tag{23}$$

Also, E_b represents the average bit energy, i.e.,

$$E_b = 2\beta \mathrm{E}[x_k^2] \tag{24}$$

and Ω is a constant dependent upon the chaotic sequence, i.e.,

$$\Omega = \frac{\mathrm{var}[x_k^2]}{\mathrm{E}^2[x_k^2]}. \tag{25}$$

Note that the BER expression obtained in (22) is independent of j, indicating that all users are having the same BER performance.

Unlike the multiple-access technique in [21] whose operation relies on specific frame structures, the proposed PMA-DCSK scheme eliminates the frame structures altogether and enables each bit of information to be sent within one bit duration. Moreover, the level of interference between users is similar. As in the single-user P-DCSK case, the data security is improved because the bit rate or frame rate cannot be determined from the frequency spectra of the signals.

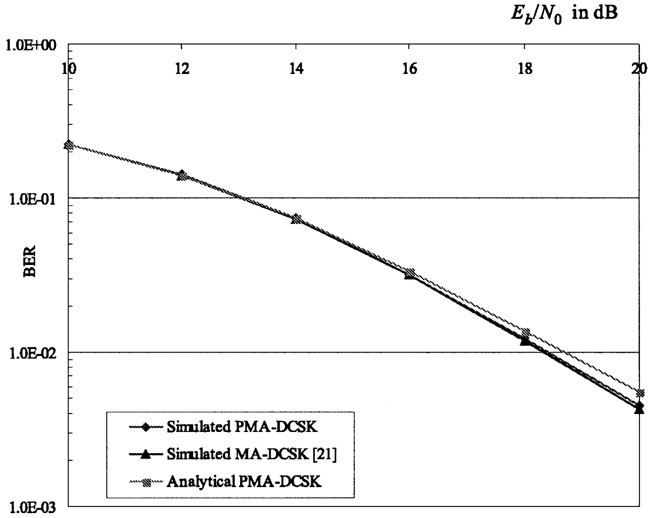


Fig. 8. Simulated and analytical BERs of MA-DCSK systems. Spreading factor $2\beta = 200$ and $N = 3$.

B. Computer Simulations and Discussions

In this section the performance of the proposed PMA-DCSK digital communication system is studied by computer simulations. We assume that the cubic map (21) is used by all users to generate the chaotic sequences, each with a different initial condition. For this map, it can be shown that

$$\mathrm{E}[x_k^2] = 0.5 \tag{26}$$

$$\mathrm{var}[x_k^2] = 0.125. \tag{27}$$

The analytical BER can thus be obtained by substituting (26) and (27) into (22) with appropriate values of spreading factor, number of users, and noise power spectral density.

The relevant BERs for the DCSK systems are shown in Figs. 8–10. From Fig. 8, we clearly see that the analytical and simulated BERs are in very good agreement for a spreading factor of 200, where the assumption of normal distribution of the conditional correlator output holds well. Also, the PMA-DCSK system achieves similar performance as that of the MA-DCSK system [21].

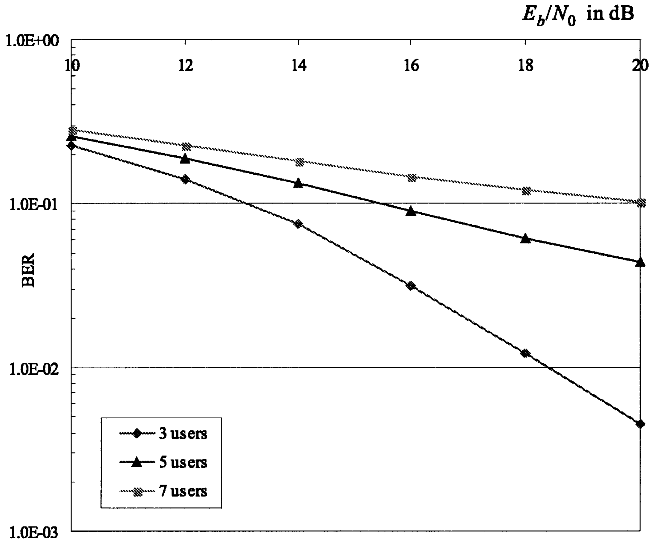


Fig. 9. Simulated BERs versus E_b/N_0 for the PMA-DCSK system. Number of users N =3, 5, and 7. Spreading factor $2\beta = 200$.

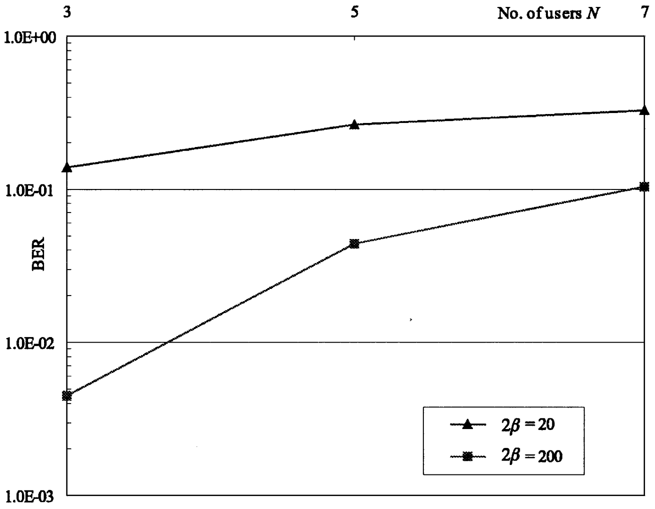


Fig. 10. Simulated BERs versus number of users N for the PMA-DCSK system. Spreading factor $2\beta = 20$ and 200. $E_b/N_0 = 20$ dB.

V. Conclusion

In this paper, we have shown that in the conventional DCSK system, the information on the bit rate can be derived easily from the transmitted signal samples. To remove this loophole from eavesdropping, we have proposed a permutation-based scheme for use with DCSK (P-DCSK). Compared with the conventional DCSK technique, additional transformation and inverse transformation are required at the transmitters and receivers. In our study, a simple permutation is performed on each signal block (reference and data samples) before transmission. At the receiving end, a reverse permutation is performed to recover the original signal block. By employing permutation, the similarity between the reference and data samples is destroyed. Thus, data security is enhanced and the bit rate is not readily detected by inspecting the signal in the frequency domain.

We also extend the P-DCSK technique to a multiple-access environment (PMA-DCSK). By appropriately assigning different permutation pairs to different users, the inter-user interference can be minimized. Compared with a previously proposed multiple-access technique [21], the PMA-DCSK scheme ensures that the transmission of the signal block for one symbol is confined to one symbol duration for all users. Also, there is no need to assign different frame periods for different users. As a consequence, users do not have to wait for half of the frame before demodulation can commence. Simulation results indicate that both systems have very similar bit error performance. Similar to the single-user case, the similarity between the reference and data samples are removed, and data security is therefore enhanced. It should be noted that although the proposed PMA-DCSK scheme has been studied with the time slots being synchronized among all participating users, it is anticipated that the interference between users will not vary too much even when the time slots are not synchronized. Thus, the BER performance should not differ substantially from that found analytically.

Appendix A
Construction of Permutation Matrices $\boldsymbol{P}_{2\beta}^{(i)}$

In this appendix, we illustrate a simple method to construct the permutation matrices $\boldsymbol{P}_{2\beta}^{(i)}$ based on a random permutation matrix and a "shifting" matrix. A permutation matrix is a square matrix in which the elements are either "0" or "1" and there is exactly one "1" in each row and in each column [22]. Define $\boldsymbol{R}_\beta$ as a random permutation matrix of size $\beta \times \beta$ and $\boldsymbol{A}_\beta$ as the "shifting" matrix of size $\beta \times \beta$ where

$$\boldsymbol{A}_\beta = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \ddots & \ddots & \ddots & 1 \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix}. \tag{28}$$

Note that the consequence of multiplying $\boldsymbol{A}_\beta$ to an array $(x_1\ x_2\ \cdots\ x_\beta) k$ times is equivalent to shifting the elements in the array to the right k times with the overflown elements being re-inserted from the left. In other words

$$\begin{aligned}(x_1\ x_2\ \cdots\ x_\beta)\boldsymbol{A}_\beta^k \\ = (x_{\beta-k+1}\ x_{\beta-k+2}\ \cdots\ x_\beta\ x_1\ x_2\ \cdots\ x_{\beta-k}).\end{aligned} \tag{29}$$

Now, the permutation matrix for user i can be chosen as

$$\boldsymbol{P}_{2\beta}^{(i)} = \begin{pmatrix} \boldsymbol{I}_\beta & \boldsymbol{0}_\beta \\ \boldsymbol{0}_\beta & \boldsymbol{R}_\beta \boldsymbol{A}_\beta^i \end{pmatrix} \tag{30}$$

where $\boldsymbol{I}_\beta$ and $\boldsymbol{0}_\beta$ are the identity matrix and zero matrix, respectively, of size $\beta \times \beta$. The permutation matrix $\boldsymbol{P}_{2\beta}^{(i,j)}$ in (20) can now be rewritten as

$$\boldsymbol{P}_{2\beta}^{(i,j)} = \begin{pmatrix} \boldsymbol{I}_\beta & \boldsymbol{0}_\beta \\ \boldsymbol{0}_\beta & \boldsymbol{R}_\beta \boldsymbol{A}_\beta^{i-j} \boldsymbol{R}_\beta^T \end{pmatrix}. \tag{31}$$

It can be readily shown that the diagonal elements of $\boldsymbol{R}_\beta \boldsymbol{A}_\beta^{i-j} \boldsymbol{R}_\beta^T$ are all zeros when $i \neq j$. Thus, the nonzero elements in the λth ($\lambda = 1, 2, \ldots, \beta$) and $(\lambda + \beta)$th rows in $\boldsymbol{P}_{2\beta}^{(i,j)}$ will not differ by β columns, and a low inter-user interference is achieved.

APPENDIX B
DERIVATION OF BER

In this appendix, we derive the analytical BERof the proposed PMA-DCSK system. All symbols are defined as in Section IV-A and in Appendix A.

Consider the lth received signal block of the jth user. When this block undergoes an inverse transformation, the output block is obtained by substituting (15), (30) and (31) into (19), i.e., as shown in (32) at the bottom of the page. When $\boldsymbol{r}_l^{(j)}$ is sent to the conventional DCSK demodulator of the jth user, the output of the correlator at the end of the lth bit duration, denoted by $y_l^{(j)}$, can be computed from

$$y_l^{(j)} = \left(\boldsymbol{x}_l^{(j)} + \sum_{\substack{i=1 \\ i\neq j}}^{N} \boldsymbol{x}_l^{(i)} + \Psi_{2l-2} \right) \cdot \left(\alpha_l^{(j)} \boldsymbol{x}_l^{(j)} + \sum_{\substack{i=1 \\ i\neq j}}^{N} \alpha_l^{(i)} \boldsymbol{x}_l^{(i)} \boldsymbol{R}_\beta \boldsymbol{A}_\beta^{i-j} \boldsymbol{R}_\beta^T + \Psi_{2l-1} \boldsymbol{A}_\beta^{-j} \boldsymbol{R}_\beta^T \right)^T. \tag{33}$$

Without loss of generality, we consider the probability of error for the first symbol, i.e., $l = 1$. For brevity, the subscripts of the variables $y_l^{(j)}$, $\boldsymbol{x}_l^{(i)}$ and $\alpha_l^{(i)}$ are omitted. The input to the threshold detector at the end of the first symbol duration, now denoted by $y^{(j)}$, is given by

$$\begin{aligned} y^{(j)} = & \alpha^{(j)} \boldsymbol{x}^{(j)} \left(\boldsymbol{x}^{(j)} \right)^T + \sum_{\substack{i=1 \\ i\neq j}}^{N} \alpha^{(i)} \boldsymbol{x}^{(j)} \boldsymbol{R}_\beta \boldsymbol{A}_\beta^{j-i} \boldsymbol{R}_\beta^T \left(\boldsymbol{x}^{(i)} \right)^T \\ & + \alpha^{(j)} \sum_{\substack{i=1 \\ i\neq j}}^{N} \boldsymbol{x}^{(i)} (\boldsymbol{x}^{(j)})^T \\ & + \sum_{\substack{n=1 \\ n\neq j}}^{N} \sum_{\substack{i=1 \\ i\neq j}}^{N} \alpha^{(i)} \boldsymbol{x}^{(n)} \boldsymbol{R}_\beta \boldsymbol{A}_\beta^{j-i} \boldsymbol{R}_\beta^T \left(\boldsymbol{x}^{(i)} \right)^T \\ & + \sum_{i=1}^{N} \boldsymbol{x}^{(i)} \boldsymbol{R}_\beta \boldsymbol{A}_\beta^{j} \Psi_1^T + \sum_{i=1}^{N} \alpha^{(i)} \Psi_0 \boldsymbol{R}_\beta \boldsymbol{A}_\beta^{j-i} \boldsymbol{R}_\beta^T \left(\boldsymbol{x}^{(i)} \right)^T \\ & + \Psi_0 \boldsymbol{R}_\beta \boldsymbol{A}_\beta^{j} \Psi_1^T \\ = & \alpha^{(j)} \boldsymbol{x}^{(j)} \left(\boldsymbol{x}^{(j)} \right)^T + \sum_{\substack{i=1 \\ i\neq j}}^{N} \alpha^{(i)} \boldsymbol{x}^{(j)} \left(\boldsymbol{z}^{(i,j)} \right)^T \\ & + \alpha^{(j)} \sum_{\substack{i=1 \\ i\neq j}}^{N} \boldsymbol{x}^{(i)} \left(\boldsymbol{x}^{(j)} \right)^T \\ & + \sum_{\substack{n=1 \\ n\neq j}}^{N} \sum_{\substack{i=1 \\ i\neq j}}^{N} \alpha^{(i)} \boldsymbol{x}^{(n)} \left(\boldsymbol{z}^{(i,j)} \right)^T + \sum_{i=1}^{N} \boldsymbol{x}^{(i)} \left(\Phi^{(j)} \right)^T \\ & + \sum_{i=1}^{N} \alpha^{(i)} \Psi_0 \left(\boldsymbol{z}^{(i,j)} \right)^T + \Psi_0 \left(\Phi^{(j)} \right)^T \end{aligned} \tag{34}$$

where

$$\boldsymbol{z}^{(i,j)} = \left(z_1^{(i,j)} \;\; z_2^{(i,j)} \;\; \cdots \;\; z_\beta^{(i,j)} \right) = \boldsymbol{x}^{(i)} \boldsymbol{R}_\beta \boldsymbol{A}_\beta^{i-j} \boldsymbol{R}_\beta^T \tag{35}$$

$$\Phi^{(j)} = \left(\phi_1^{(j)} \;\; \phi_2^{(j)} \;\; \cdots \;\; \phi_\beta^{(j)} \right) = \Psi_1 \boldsymbol{A}_\beta^{-j} \boldsymbol{R}_\beta^T. \tag{36}$$

Note that the elements in $\boldsymbol{z}^{(i,j)}$ and $\Phi^{(j)}$ are permutations of the elements in $\boldsymbol{x}^{(i)}$ and Ψ_1, respectively.

Suppose "+1" is transmitted for user j, i.e., $\alpha^{(j)} = +1$. Then, (34) becomes

$$\begin{aligned} & y^{(j)} \Big| \left(\alpha^{(j)} = +1 \right) \\ & = \underbrace{U^{(j,j)}}_{\text{required signal}} \\ & \quad \underbrace{+ \sum_{\substack{i=1 \\ i\neq j}}^{N} \alpha^{(i)} V^{(j,i,j)} + \sum_{\substack{i=1 \\ i\neq j}}^{N} U^{(i,j)} + \sum_{\substack{n=1 \\ n\neq j}}^{N} \sum_{\substack{i=1 \\ i\neq j}}^{N} \alpha^{(i)} V^{(n,i,j)}}_{\text{inter-user interference}} \\ & \quad \underbrace{+ \sum_{i=1}^{N} W^{(i,j)} + X^{(j,j)} + \sum_{\substack{i=1 \\ i\neq j}}^{N} \alpha^{(i)} X^{(i,j)} + Y^{(j)}}_{\text{noise}} \end{aligned} \tag{37}$$

where

$$U^{(i,j)} = \boldsymbol{x}^{(i)} \left(\boldsymbol{x}^{(j)} \right)^T = \sum_{k=1}^{\beta} x_k^{(i)} x_k^{(j)} \tag{38}$$

$$\begin{aligned} \boldsymbol{r}_l^{(j)} = & \left(\boldsymbol{x}_l^{(j)} \quad \alpha_l^{(j)} \boldsymbol{x}_l^{(j)} \right) + \left(\sum_{\substack{i=1 \\ i\neq j}}^{N} \boldsymbol{x}_l^{(i)} \quad \sum_{\substack{i=1 \\ i\neq j}}^{N} \alpha_l^{(i)} \boldsymbol{x}_l^{(i)} \boldsymbol{R}_\beta \boldsymbol{A}_\beta^{i-j} \boldsymbol{R}_\beta^T \right) + \left(\Psi_{2l-2} \quad \Psi_{2l-1} \boldsymbol{A}_\beta^{-j} \boldsymbol{R}_\beta^T \right) \\ = & \left(\boldsymbol{x}_l^{(j)} + \sum_{\substack{i=1 \\ i\neq j}}^{N} \boldsymbol{x}_l^{(i)} + \Psi_{2l-2} \quad \alpha_l^{(j)} \boldsymbol{x}_l^{(j)} + \sum_{\substack{i=1 \\ i\neq j}}^{N} \alpha_l^{(i)} \boldsymbol{x}_l^{(i)} \boldsymbol{R}_\beta \boldsymbol{A}_\beta^{i-j} \boldsymbol{R}_\beta^T + \Psi_{2l-1} \boldsymbol{A}_\beta^{-j} \boldsymbol{R}_\beta^T \right) \end{aligned} \tag{32}$$

$$V^{(n,\,i,\,j)} = \boldsymbol{x}^{(n)} \left(\boldsymbol{z}^{(i,\,j)}\right)^T = \sum_{k=1}^{\beta} x_k^{(n)} z_k^{(i,\,j)} \tag{39}$$

$$W^{(i,\,j)} = \boldsymbol{x}^{(i)} \left(\Phi^{(j)}\right)^T = \sum_{k=1}^{\beta} x_k^{(i)} \phi_k^{(j)} \tag{40}$$

$$X^{(i,\,j)} = \Psi_0 \left(\boldsymbol{z}^{(i,\,j)}\right)^T = \sum_{k=1}^{\beta} \xi_k z_k^{(i,\,j)} \tag{41}$$

$$Y^{(j)} = \Psi_0 \left(\Phi^{(j)}\right)^T = \sum_{k=1}^{\beta} \xi_k \phi_k^{(j)}. \tag{42}$$

Notice that the input to the detector consists of three components, namely required signal, inter-user interference and noise. The mean value of $y^{(j)}|(\alpha^{(j)} = +1)$ is given by

$$\begin{aligned}
&\mathrm{E}\left[y^{(j)}\Big|\left(\alpha^{(j)} = +1\right)\right] \\
&\quad = \mathrm{E}\left[U^{(j,\,j)}\right] + \sum_{\substack{i=1\\ i\neq j}}^{N} \alpha^{(i)}\mathrm{E}\left[V^{(j,\,i,\,j)}\right] + \sum_{\substack{i=1\\ i\neq j}}^{N} \mathrm{E}\left[U^{(i,\,j)}\right] \\
&\qquad + \sum_{\substack{n=1\\ n\neq j}}^{N} \sum_{\substack{i=1\\ i\neq j}}^{N} \alpha^{(i)}\mathrm{E}\left[V^{(n,\,i,\,j)}\right] + \sum_{i=1}^{N} \mathrm{E}\left[W^{(i,\,j)}\right] \\
&\qquad + \mathrm{E}\left[X^{(j,\,j)}\right] + \sum_{\substack{i=1\\ i\neq j}}^{N} \alpha^{(i)}\mathrm{E}\left[X^{(i,\,j)}\right] + \mathrm{E}\left[Y^{(j)}\right] \\
&\quad = \mathrm{E}\left[U^{(j,\,j)}\right] + \sum_{\substack{i=1\\ i\neq j}}^{N} \alpha^{(i)}\mathrm{E}\left[V^{(j,\,i,\,j)}\right] + \sum_{\substack{i=1\\ i\neq j}}^{N} \mathrm{E}\left[U^{(i,\,j)}\right] \\
&\qquad + \sum_{\substack{n=1\\ n\neq j}}^{N} \sum_{\substack{i=1\\ i\neq j}}^{N} \alpha^{(i)}\mathrm{E}\left[V^{(n,\,i,\,j)}\right]
\end{aligned} \tag{43}$$

where $\mathrm{E}[\psi]$ denotes the mean value of ψ. The last equality holds because $\mathrm{E}[\xi_k]$ and $\mathrm{E}[\phi_k^{(j)}]$ are both zero. The variance of $y^{(j)}|(\alpha^{(j)} = +1)$ is found from [23]

$$\begin{aligned}
&\mathrm{var}\left[y^{(j)}\Big|\left(\alpha^{(j)} = +1\right)\right] \\
&\quad = \sum_{i=1}^{N} \mathrm{var}\left[U^{(i,\,j)}\right] + \sum_{n=1}^{N} \sum_{\substack{i=1\\ i\neq j}}^{N} \mathrm{var}\left[V^{(n,\,i,\,j)}\right] \\
&\qquad + \sum_{i=1}^{N} \mathrm{var}\left[W^{(i,\,j)}\right] + \sum_{i=1}^{N} \mathrm{var}\left[X^{(i,\,j)}\right] + \mathrm{var}\left[Y^{(j)}\right] \\
&\qquad + \sum_{\substack{C\\ C\neq D}} \sum_{D} \mathrm{cov}[C,\,D]
\end{aligned} \tag{44}$$

where $C, D \in \{U^{(i,\,j)}(i = 1, \ldots, N);\ \alpha^{(i)}V^{(n,\,i,\,j)}\ (n = 1, \ldots, N;\ i = 1, \ldots, j-1,\ j+1, \ldots, N);\ W^{(i,\,j)}\ (i = 1, \ldots, N);\ X^{(j,\,j)};\ \alpha^{(i)}X^{(i,\,j)}\ (i = 1, \ldots, j-1, j+1, \ldots, N);\ Y^{(j)}\}$, $\mathrm{var}[\psi]$ denotes the variance of ψ, and $\mathrm{cov}[C,\,D]$ represents the covariance of C and D defined as

$$\mathrm{cov}[C,\,D] = \mathrm{E}[CD] - \mathrm{E}[C]\mathrm{E}[D]. \tag{45}$$

We assume that all users use the cubic map

$$x_{k+1} = g(x_k) = 4x_k^3 - 3x_k \tag{46}$$

to generate the chaotic sequences, and each uses a different initial condition. With this map, the mean value of each chaotic sequence is zero [17]. Also, it can be readily shown that

$$\mathrm{E}\left[U^{(i,\,j)}\right] = \begin{cases} \beta\mathrm{E}[x_k^2], & \text{if } i = j \\ 0, & \text{otherwise} \end{cases} \tag{47}$$

$$\begin{aligned}
\mathrm{E}\left[V^{(n,\,i,\,j)}\right] = 0, \qquad & n = 1, \ldots, N; \\
& i = 1, \ldots, j-1;\ j+1, \ldots, N.
\end{aligned} \tag{48}$$

Furthermore, the variances of the terms in (38)–(42) are given by

$$\mathrm{var}\left[U^{(i,\,j)}\right] = \begin{cases} \beta\mathrm{var}[x_k^2], & \text{if } i = j \\ \beta\mathrm{E}^2[x_k^2], & \text{otherwise} \end{cases} \tag{49}$$

$$\mathrm{var}\left[V^{(n,\,i,\,j)}\right] = \begin{cases} \beta\mathrm{E}^2[x_k^2], & \text{for } i \neq j, i \neq n \\ \dfrac{\beta^2}{\beta - 1}\,\mathrm{E}^2[x_k^2] \approx \beta\mathrm{E}^2[x_k^2], & \text{for } i \neq j, i = n \end{cases} \tag{50}$$

$$\mathrm{var}\left[W^{(i,\,j)}\right] = \beta N_0 \mathrm{E}[x_k^2]/2 \tag{51}$$

$$\mathrm{var}\left[X^{(i,\,j)}\right] = \beta N_0 \mathrm{E}[x_k^2]/2 \tag{52}$$

$$\mathrm{var}\left[Y^{(j)}\right] = \beta N_0^2/4 \tag{53}$$

and the covariance terms in (44) can be shown to be zero. Thus, (43) and (44) can be simplified to

$$\mathrm{E}\left[y^{(j)}\Big|\left(\alpha^{(j)} = +1\right)\right] = \beta\mathrm{E}[x_k^2] \tag{54}$$

$$\begin{aligned}
&\mathrm{var}\left[y^{(j)}\Big|\left(\alpha^{(j)} = +1\right)\right] \\
&\quad \approx \beta\mathrm{var}[x_k^2] + (N-1)\beta\mathrm{E}^2[x_k^2] + (N^2 - N)\beta\mathrm{E}^2[x_k^2] \\
&\qquad + N\beta N_0\mathrm{E}[x_k^2]/2 + N\beta N_0\mathrm{E}[x_k^2]/2 + \beta N_0^2/4 \\
&\quad = \beta\mathrm{var}[x_k^2] + (N^2 - 1)\beta\mathrm{E}^2[x_k^2] + N\beta N_0\mathrm{E}[x_k^2] + \beta N_0^2/4.
\end{aligned} \tag{55}$$

Likewise, we can find the mean and variance of $y^{(j)}$ given a "−1" has been sent. Denote the respective mean and variance by $\mathrm{E}[y^{(j)}|(\alpha^{(j)} = -1)]$ and $\mathrm{var}[y^{(j)}|(\alpha^{(j)} = -1)]$. Using the aforementioned results, it can be easily shown that

$$\mathrm{E}\left[y^{(j)}\Big|\left(\alpha^{(j)} = -1\right)\right] = -\mathrm{E}\left[y^{(j)}\Big|\left(\alpha^{(j)} = +1\right)\right] \tag{56}$$

$$\mathrm{var}\left[y^{(j)}\Big|\left(\alpha^{(j)} = -1\right)\right] = \mathrm{var}\left[y^{(j)}\Big|\left(\alpha^{(j)} = +1\right)\right]. \tag{57}$$

$$\begin{aligned}
\mathrm{BER}^{(j)} &= \tfrac{1}{2}\mathrm{Prob}\left(y^{(j)} \le 0 \middle| \left(\alpha^{(j)} = +1\right)\right) + \tfrac{1}{2}\mathrm{Prob}\left(y^{(j)} > 0 \middle| \left(\alpha^{(j)} = -1\right)\right) \\
&= \frac{1}{4}\,\mathrm{erfc}\left(\frac{\mathrm{E}[y^{(j)}|(\alpha^{(j)}=+1)]}{\sqrt{2\mathrm{var}[y^{(j)}|(\alpha^{(j)}=+1)]}}\right) + \frac{1}{4}\,\mathrm{erfc}\left(\frac{-\mathrm{E}[y^{(j)}|(\alpha^{(j)}=-1)]}{\sqrt{2\mathrm{var}[y^{(j)}|(\alpha^{(j)}=-1)]}}\right) \\
&= \frac{1}{2}\,\mathrm{erfc}\left(\frac{\mathrm{E}[y^{(j)}|(\alpha^{(j)}=+1)]}{\sqrt{2\mathrm{var}[y^{(j)}|(\alpha^{(j)}=+1)]}}\right) \\
&= \frac{1}{2}\,\mathrm{erfc}\left(\frac{\beta\mathrm{E}[x_k^2]}{\sqrt{2(\beta\mathrm{var}[x_k^2] + (N^2-1)\beta\mathrm{E}^2[x_k^2] + N\beta N_0\mathrm{E}[x_k^2] + \beta N_0^2/4)}}\right) \\
&= \frac{1}{2}\,\mathrm{erfc}\left(\left[\frac{2}{\beta}\left(\frac{\mathrm{E}^2[x_k^2]}{\mathrm{var}[x_k^2]}\right)^{-1} + \frac{2(N^2-1)}{\beta} + \frac{2N}{\beta}\left(\frac{\mathrm{E}[x_k^2]}{N_0}\right)^{-1} + \frac{1}{2\beta}\left(\frac{\mathrm{E}[x_k^2]}{N_0}\right)^{-2}\right]^{-\frac{1}{2}}\right) \qquad (58) \\
&= \frac{1}{2}\,\mathrm{erfc}\left(\left[\frac{2\Omega}{\beta} + \frac{2(N^2-1)}{\beta} + 4N\left(\frac{E_b}{N_0}\right)^{-1} + 2\beta\left(\frac{E_b}{N_0}\right)^{-2}\right]^{-\frac{1}{2}}\right) \qquad (59)
\end{aligned}$$

Since $y^{(j)}|(\alpha^{(j)} = +1)$ and $y^{(j)}|(\alpha^{(j)} = -1)$ are the sum of a large number of random variables, we may assume that both of them are approximately normal. This assumption holds better for larger spreading factors [24]. In the detection of the symbol, an error occurs if $y^{(j)} \le 0|(\alpha^{(j)} = +1)$ or $y^{(j)} > 0|(\alpha^{(j)} = -1)$. The BER for user j can thus be computed from (58) and (59) shown at the top of the page, where the complementary error function, $\mathrm{erfc}(.)$, is defined as

$$\mathrm{erfc}(\psi) \equiv \frac{2}{\sqrt{\pi}}\int_{\psi}^{\infty} e^{-\lambda^2}\, d\lambda. \qquad (60)$$

Also, E_b represents the average bit energy and is given by

$$E_b = 2\beta\mathrm{E}[x_k^2] \qquad (61)$$

and

$$\Omega = \frac{\mathrm{var}[x_k^2]}{\mathrm{E}^2[x_k^2]}. \qquad (62)$$

Note that Ω is a constant for a given chaotic sequence, regardless of the presence of any scaling factor of the sequence. This can be illustrated as follows. Suppose the chaotic sequence $\{x_k\}$ is multiplied by the factor ν before transmission and the average power of the signal is changed by ν^2 times. The value of Ω remains unchanged, i.e.,

$$\Omega = \frac{\mathrm{var}[(\nu x_k)^2]}{\mathrm{E}^2[(\nu x_k)^2]} = \frac{\mathrm{var}[\nu^2 x_k^2]}{\mathrm{E}^2[\nu^2 x_k^2]} = \frac{\nu^4\mathrm{var}[x_k^2]}{\nu^4\mathrm{E}^2[x_k^2]} = \frac{\mathrm{var}[x_k^2]}{\mathrm{E}^2[x_k^2]}. \qquad (63)$$

References

[1] L. M. Pecaro and T. L. Carroll, "Synchronization in chaotic systems," *Phys. Rev. Lett.*, vol. 64, pp. 821–824, 1990.

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

[3] K. M. Cuomo and A. V. Oppenheim, "Circuit implementation of synchronized chaos with applications to communications," *Phys. Rev. Lett.*, vol. 71, pp. 65–68, 1993.

[4] U. Parlitz, L. O. Chua, L. Kocarev, K. S. Halle, and A. Shang, "Transmission of digital signals by chaotic synchronization," *Int. J. Bifurcation Chaos*, vol. 2, pp. 973–977, 1992.

[5] 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*, vol. 40, pp. 634–642, Oct. 1993.

[6] G. Kolumbán, B. Vizvari, W. Schwarz, and A. Abel, "Differential chaos shift keying: A robust coding for chaos communications," in *Proc., 4th Int. Workshop on Nonlinear Dynamics of Electronics Systems, (NDES'96)*, Seville, Spain, June 1996, pp. 87–92.

[7] 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 and Its Applications, (NOLTA'97)*, Hawaiian Village, HI, 1997, pp. 117–120.

[8] G. Kolumbán, G. Kis, Z. Jáko, and M. P. Kennedy, "A robust modulation scheme for chaotic communications," *IEICE Trans. Fund.*, vol. E81-A, pp. 1798–1802, 1998.

[9] 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*, vol. 45, pp. 1129–1140, Nov. 1998.

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

[11] 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*, vol. 47, pp. 1673–1683, Dec. 2000.

[12] T. Schimming and M. Hasler, "Optimal detection of differential chaos shift keying," *IEEE Trans. Circuits Syst. I*, vol. 47, pp. 1712–1719, Dec. 2000.

[13] T. Yang and L. O. Chua, "Chaotic digital code-division multiple access (CDMA) communication systems," *Int. J. Bifurcation Chaos*, vol. 7, no. 12, pp. 2789–2805, 1997.

[14] G. Mazzini, G. Setti, and R. Rovatti, "Chaotic complex spreading sequences for asynchronous DS-CDMA. Part I: System modeling and results," *IEEE Trans. Circuits Syst. I*, vol. 44, pp. 937–947, Oct. 1997.

[15] ——, "Chaotic complex spreading sequences for asynchronous DS-CDMA—Part II: Some theoretical performance bounds," *IEEE Trans. Circuits Syst. I*, vol. 45, pp. 496–506, Oct. 1998.

[16] L. S. Tsimring, A. R. Volkovskii, S. C. Young, and N. F. Rulkov, "Multi-user communication using chaotic frequency modulation," in *Proc. Int. Symp. Nonlinear Theory and Its Applications, (NOLTA'01)*, Miyagi, Japan, Oct. 2001, pp. 561–564.

[17] W. M. Tam, F. C. M. Lau, C. K. Tse, and M. M. Yip, "An approach to calculating the bit error probability of a coherent chaos-shift-keying digital communication system under a noisy multi-user environment," *IEEE Trans. Circuits Syst. I*, vol. 49, pp. 210–223, Feb. 2002.

[18] G. Kolumbán, M. P. Kennedy, and G. Kis, "Multilevel differential chaos shift keying," in *Proc. 5th Int. Workshop on Nonlinear Dynamics of Electronics Systems, (NDES'97)*, Moscow, Russia, June 1997, pp. 191–196.

[19] M. P. Kennedy, G. Kolumbán, G. Kis, and Z. Jáko, "Recent advances in communicating with chaos," in *Proc. IEEE Int. Symp. Circuits and Systems, (ISCAS '98)*, vol. 4, Monterey, CA, May 1998, pp. 461–464.

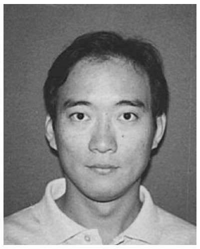
[20] Z. Jáko, G. Kis, and G. Kolumbán, "Multiple access capability of the FM-DCSK chaotic communications system," in *Proc. 8th Int. Specialist Workshop on Nonlinear Dynamics of Electronics Systems, (NDES'2000)*, Cantania, Italy, May 2000, pp. 52–55.

[21] F. C. M. Lau, M. M. Yip, C. K. Tse, and S. F. Hau, "A multiple-access technique for differential chaos shift keying," *IEEE Trans. Circuits Syst. I*, vol. 49, pp. 96–104, Jan. 2002.

[22] G. W. Stewart, *Matrix Algorithms*. Philadelphia, PA: SIAM, 1998.

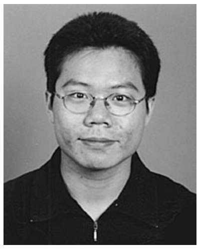
[23] S. M. Ross, *Introduction to Probability Models*, 5 ed. New York: Academic, 1993.

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



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, London, U.K., in 1989 and 1993, respectively.

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



Kai Y. Cheong received the B.Eng. (Hons.) degree in 2001 from the Department of Electronic and Information Engineering, The Hong Kong Polytechnic University, Hong Kong, where he is currently working toward the M.Phil. degree in the area of chaos-based digital communications.

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

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

Prof. Tse served as an Associate Editor of the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS PART I—FUNDAMENTAL THEORY AND APPLICATIONS, from 1999 to 2001, and since 1999, he has been an Associate Editor of the IEEE TRANSACTIONS ON POWER ELECTRONICS. 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 twice the President's Award for Achievement in Research, the Faculty's Best Researcher Award, and a few other teaching awards. Since 2002, he has been appointed as Advisory Professor by the Southwest China Normal University, Chongqing, China.