A Permutation-based Multiple Access DCSK System

Francis C.M. Lau, Kai Y. Cheong and Chi K. Tse

Department of Electronic and Information Engineering, The Hong Kong Polytechnic University,
Hunghom, Kowloon, Hong Kong SAR, China.
Phone:+852-2766-6206, Fax:+852-2362-8439
Email: encmlau@polyu.edu.hk, 01900720r@polyu.edu.hk & encktse@polyu.edu.hk

Abstract

This paper presents a method to enhance 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.

1. Introduction

A number of chaos-based communication schemes have been proposed and studied in recent years, including chaos masking [1, 2], chaotic switching or chaos-shift-keying (CSK) [3, 4], differential CSK (DCSK) [5] and frequency-modulated DCSK (FM-DCSK) [6]. Among the digital communication techniques proposed, CSK and DCSK are the most widely studied [7, 8]. 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.

In this paper, a permutation approach for enhancing the DCSK scheme is proposed. The frequency spectrum of the proposed system will be compared with that of a conventional DCSK system. The proposed DCSK scheme is also 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 multiple access DCSK scheme.

This work is supported by a research grant provided by Hong Kong Polytechnic University and also by a competitive earmarked research grant funded by the Hong Kong Research Grants Council (Grant No. PolyU5124/01E).

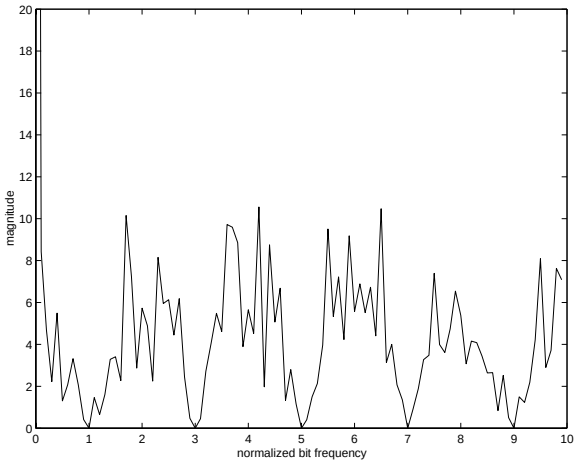

Fig. 1: Magnitude of frequency components versus normalized bit frequency for the square of a conventional DCSK signal sample.

2. Conventional Differential DCSK System

For a conventional DCSK system, the transmitted signal block during the lth bit duration is given by $\boldsymbol{s}_l = (\boldsymbol{x}_l \quad \alpha_l \boldsymbol{x}_l)$ where $\boldsymbol{x}_l = (x_{2\beta(l-1)+1} \quad x_{2\beta(l-1)+2} \quad \cdots \quad x_{2\beta(l-1)+\beta})$ is the reference sample, $\alpha_l \in \{-1, +1\}$ denotes the lth transmitted symbol, and 2β is the spreading factor defined as the number of chaotic samples sent for each binary symbol.

We analyse the frequency spectrum of a 10-bit DCSK signal sample. We square the DCSK signal sample and plot the magnitude spectrum. From Fig. 1, 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 resul-

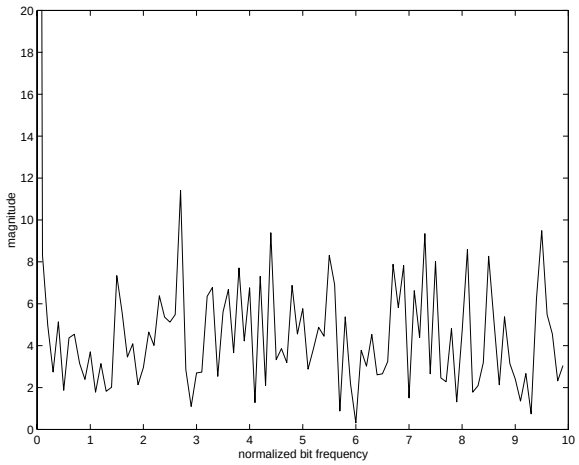

Fig. 3: Magnitude of frequency components versus normalized bit frequency for the square of a permutation-based DCSK signal sample.

tant 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 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.

3. Permutation-Based DCSK System

Fig. 2 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 $\boldsymbol{u}_l = F(\boldsymbol{s}_l)$. At the receiver, each incoming block $\boldsymbol{v}_l$ will first undergo an inverse transformation $G = F^{-1}$ to retrieve an output block $\boldsymbol{r}_l$, i.e., $\boldsymbol{r}_l = G(\boldsymbol{v}_l)$. 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. That is to say, the transformation and inverse transformation are given by, respectively, $F(\boldsymbol{s}_l) = \boldsymbol{s}_l \boldsymbol{P}_{2\beta}$ and $G(\boldsymbol{v}_l) = F^{-1}(\boldsymbol{v}_l) = \boldsymbol{v}_l(\boldsymbol{P}_{2\beta})^{-1} = \boldsymbol{v}_l(\boldsymbol{P}_{2\beta})^T$ where $\boldsymbol{P}_{2\beta}$ is a $2\beta \times 2\beta$ permutation matrix [10] in which the elements are either "0" or "1" and there is exactly one "1" in each row and in each column.

The frequency spectrum of the square of the P-DCSK signal sample is plotted in Fig. 3. It can be seen that 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.

4. Permutation-Based Multiple Access DCSK System

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

Fig. 4 depicts the block diagram of a permutation-based multiple access DCSK (PMA-DCSK) system. Denote the lth transmitted symbol of user i by $\alpha_l^{(i)}$. The corresponding signal block will be given by $\boldsymbol{s}_l^{(i)} = (\boldsymbol{x}_l^{(i)} \quad \alpha_l^{(i)} \boldsymbol{x}_l^{(i)})$ where $\boldsymbol{x}_l^{(i)} = (x_{2\beta(l-1)+1}^{(i)} \quad x_{2\beta(l-1)+2}^{(i)} \quad \cdots \quad x_{2\beta(l-1)+\beta}^{(i)})$ 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 $\boldsymbol{u}_l^{(i)} = F_i(\boldsymbol{s}_l^{(i)}) = \boldsymbol{s}_l^{(i)} \boldsymbol{P}_{2\beta}^{(i)}$ 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.,

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

At the jth receiver, denote the lth received signal block by $\boldsymbol{v}_l = \boldsymbol{u}_l + (\Psi_{2l-2} \quad \Psi_{2l-1})$. 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.,

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

where

$$\boldsymbol{P}_{2\beta}^{(i,j)} = \boldsymbol{P}_{2\beta}^{(i)} (\boldsymbol{P}_{2\beta}^{(j)})^T. \tag{3}$$

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 ($\lambda =$

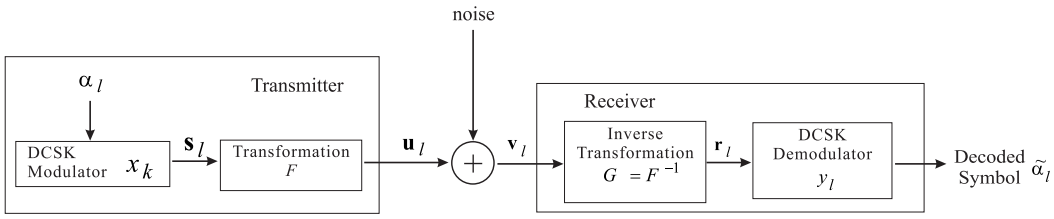

Fig. 2: Proposed permutation-based DCSK communication system.

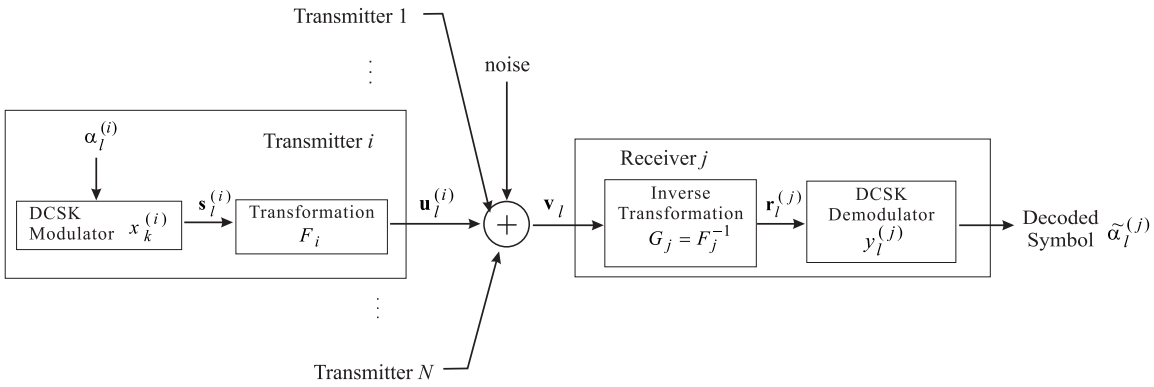

Fig. 4: Proposed multiple access DCSK communication system.

$1, 2, \ldots, \beta)$ 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. There are many ways to choose the permutation matrices such that the aforementioned condition is satisfied. One simple example, based on a random permutation matrix and a "shifting" matrix, is described in the appendix. We assume that all users use the cubic map

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

to generate the chaotic sequences, and each uses a different initial condition. Based on the permutation matrices constructed in the appendix, the analytical bit error rate can be found as

$$\mathrm{BER}^{(j)} = \frac{1}{2}\mathrm{erfc}\left(\left[\frac{2\Psi}{\beta} + \frac{2(N^2-1)}{\beta} + 4N\left(\frac{E_b}{N_0}\right)^{-1} + 2\beta\left(\frac{E_b}{N_0}\right)^{-2}\right]^{-\frac{1}{2}}\right) \tag{5}$$

where erfc(.) is the complementary error function, $E_b = 2\beta \mathrm{E}[x_k^2]$ represents the average bit energy, and $\Psi = \mathrm{var}[x_k^2]/\mathrm{E}^2[x_k^2]$ is a constant dependent upon the chaotic sequence. Note that the BER expression obtained in (5) is independent of j, indicating that all users are having the same BER performance.

The performance of the proposed permutation-based multiple access DCSK (PMA-DCSK) digital communication system is also studied by computer simulations. For the cubic map (4), it can be shown that

$$\mathrm{E}[x_k^2] = 0.5 \tag{6}$$

$$\mathrm{var}[x_k^2] = 0.125. \tag{7}$$

The analytical bit error rate (BER) can thus be obtained by substituting (6) and (7) into (5) with appropriate values of spreading factor, number of users and noise power spectral density. From Fig. 5, 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 [9].

5. Conclusion

In this paper, we have shown that in the conventional differential chaos-shift-keying (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.

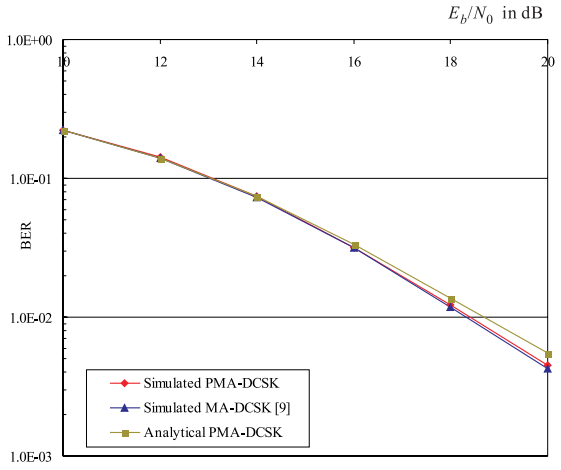

Fig. 5: Simulated and analytical BERs of multiple access DCSK systems. Spreading factor 2β = 200 and $N = 3$.

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 [9], 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. 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.

Appendix: 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 [10] . 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

$$\boldsymbol{A}_\beta = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \ddots & \ddots & \ddots & 1 \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix}. \tag{8}$$

Note that

$$\begin{aligned} & (x_1 \;\; x_2 \;\; \ldots \;\; x_\beta)\boldsymbol{A}_\beta^k \\ = \;& (x_{\beta-k+1} \;\; x_{\beta-k+2} \;\; \ldots \;\; x_\beta \;\; x_1 \;\; x_2 \;\; \ldots \;\; x_{\beta-k}). \end{aligned} \tag{9}$$

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

$$\boldsymbol{P}_{2\beta}^{(i)} = \begin{pmatrix} \boldsymbol{I}_\beta & \boldsymbol{0}_\beta \\ \boldsymbol{0}_\beta & \boldsymbol{R}_\beta \boldsymbol{A}_\beta^i \end{pmatrix} \tag{10}$$

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 (3) can now be re-written as

$$\boldsymbol{P}_{2\beta}^{(i,j)} = \begin{pmatrix} \boldsymbol{I}_\beta & \boldsymbol{0}_\beta \\ \boldsymbol{0}_\beta & \boldsymbol{R}_\beta \boldsymbol{A}_\beta^{i-j} \boldsymbol{R}_\beta^T \end{pmatrix}. \tag{11}$$

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 non-zero 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.

References

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

[2] 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.

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

[4] 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. on Circuits and Systems II*, vol. 40, pp. 634–642, 1993.

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

[6] G. Kolumbán, G. Kis, M.P. Kennedy and Z. Jáko, "FM-DCSK: a new and robust solution to chaos communications," *Proc., International Symposium on Nonlinear Theory and Its Applications*, (NOLTA'97), Hawaii, pp. 117–120, 1997.

[7] 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. on Circ. Syst. I*, vol. 45, no. 11, pp. 1129–1140, 1998.

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

[9] 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. on Circuits and Systems I*, vol. 49, no. 1, pp. 96–104, Jan. 2002.

[10] G.W. Stewart, *Matrix Algorithms*, Philadelphia: Society for Industrial and Applied Mathematics, 1998.