Multibit-Parallel Scrambling Techniques for Distributed Sample Scrambling

Seok Chang Kim, Nonmember and Byeong Gi Lee, Member

SUMMARY In this paper, we develop parallel scrambling techniques for the distributed sample scrambling (DSS), which are directly applicable to the bit- and multibit-interleaved multiplexing environments. We first consider how to realize PSRGs, parallel samplings and parallel corrections for the multibit-parallel DSS (MPDSS), which are the fundamental problems in realizing the MPDSS scramblers and descramblers. The results are summarized in three sets of theorems, and a corollary is attached to each theorem to specifically handle the case of the parallel DSS (PDSS). The theorems and corollaries are supported by examples that demonstrate the relevant MPDSS scramblers and descramblers.

key words: parallel scrambling, distributed sample scrambling (DSS), parallel shift register generator, parallel sampling, parallel correction

1. Introduction

In digital transmission systems, in general, multiple of base-rate signals are multiplexed bit- or byte-interleaving based and then scrambled to form a single transmission signal, which is descrambled and demultiplexed in the receiving terminal. Depending on the synchronization methods, scrambling techniques are classified into three categories—the self-synchronous scrambling (SSS) [1], the frame synchronous scrambling (FSS) [2], and the distributed sample scrambling (DSS) [3]. Among the three scrambling techniques, the DSS is the most recently introduced scrambling technique that acquires synchronization by utilizing distributed samples taken from the shift register generators (SRG) in the scrambler and the descrambler.

As transmission rates rapidly grew up to the gigabit-per-second (Gbps) range in recent lightweight transmission, the concept of parallel scrambling has been introduced to enable the scrambling at a low-speed base-rate [4]. In the case of the SSS, parallel SSS (PSSS) technique is available for the bit-interleaved multiplexing environment [4]; and in the FSS case, parallel FSS (PFSS) and multibit-parallel FSS (MPFSS) techniques are available respectively for the bit- and the multibit-interleaved multiplexing environments [4]–[6].

In the case of the DSS, a parallel DSS (PDSS) technique was introduced in Ref. [7] for use in parallel scrambling of the cell-based asynchronous transfer mode (ATM) transmission signal [8]. However, this PDSS technique is applicable only to some limited cases in which two samples are simultaneously transmitted in parallel. Furthermore, no multibit-parallel DSS (MPDSS) technique is yet reported in literature. Therefore, in this paper we are going to introduce an MPDSS technique that renders a generalized MPDSS technique which includes the PDSS technique in Ref. [7] as a special case. For this, we will employ the sequence space, the SRG, and the parallel SRG (PSRG) theories [6], [9], so that we can realize the PSRGs, the parallel samplings and the parallel corrections for the MPDSS in a systematic manner. The developed MPDSS techniques will then completely solve the scrambling speed problem in the transmission systems employing the DSS, whose most typical example being the cell-based ATM transmission system.

We will first consider fundamentals of the sequence space, the SRG and the PSRG theories for use in developing multibit-parallel DSS in Sect. 2. Then, we will discuss how to realize the PSRGs, the parallel samplings and the parallel corrections for the MPDSS respectively in Sects. 3 to 5, demonstrating the discussions through examples in each section.

2. Fundamentals for Multibit-Parallel DSS

A sequence space $V[\Psi(x)]$, which is characterized by the characteristic polynomial $\Psi(x) = \sum_{i=0}^{L} \psi_i x^i$ for the binary coefficients $\psi_i$, $i=0, 1, \ldots, L$ with $\psi_0 = \psi_L = 1$, is an $L$-dimensional vector space whose elements are sequences $\{ s_k \}$ satisfying the recurrent relation $\sum_{i=0}^{L} \psi_i s_{k+i} = 0$ for all $k=0, 1, \ldots$.

For an SRG with the state transition matrix $T$ and the generating vector $h$, the scrambling space $V[T, h]$ refers to the set whose elements are the scrambling sequences $\{ s_k \}$'s obtained by varying the initial state vectors $d_0$'s, which is identical to the sequence space $V[\Psi T_h(x)]$ for the lowest-degree polynomial $\Psi T_h(x)$ meeting the relation $h^T \Psi T_h(T) = 0$.

If a sample $z$ is taken at the sampling time $\alpha$ from the scrambling sequence $\{ s_k \}$ generated by an SRG...
with the state transition matrix $T$ and the generating vector $h$, then this sample is identical to the sample taken at a time $\gamma$ using the sampling vector

$$\mathbf{v} = (T')^{\gamma-1} \cdot \mathbf{h}.$$  

(1)

For a serial sequence $\{s_k\}$, if a PSRG generates $N$ parallel sequences $\{s^j_k\}$, $j=0, 1, \ldots, N-1$, such that

$$
\begin{align*}
\{s^0_k\} &= \{s_0, s_1, \ldots, s_{M-1}; s_{MN}, s_{MN+1}, \ldots, s_{M(N+1)-1}; \ldots\}, \\
\{s^j_k\} &= \{s_{Mj}, s_{Mj+1}, \ldots, s_{M(N+1)-1}; s_{M(N+1)+1}; s_{M(N+1)+2}; \ldots, s_{M(N+2)-1}; \ldots\}, \\
&\quad \quad \vdots \\
\{s^{N-1}_k\} &= \{s_{(N-1)M}, s_{(N-1)M+1}; \ldots; s_{MN-1}; s_{MN}; s_{MN+1}; \ldots\},
\end{align*}
$$

(2)

then this PSRG is called an $(M, N)$ PSRG for the serial sequence $\{s_k\}$, and a minimum-length PSRG is called a minimal $(M, N)$ PSRG.

If the $N$ parallel sequences $\{s^j_k\}$, $j=0, 1, \ldots, N-1$, have the expression $s^j_k = \mathbf{E}_{\Psi_m(x)} \mathbf{s}_j$, for initial vectors $\mathbf{s}_j$'s and the elementary basis vector $\mathbf{E}_{\Psi_m(x)}$ on their minimal space $V[\Psi_m(x)]$, then for a nonsingular matrix $Q$ the PSRG with the state transition matrix $T$, the initial state vector $d_0$ and the generating vectors $h_j$'s such that

$$
\begin{align*}
T &= Q \cdot A_{\Psi_m(x)} \cdot Q^{-1}, \\
d_0 &= Q \cdot d_0, \\
h_j &= (Q')^{-1} \cdot s_j, \quad j = 0, 1, \ldots, N-1,
\end{align*}
$$

is a minimal PSRG generating the parallel sequences $\{s^j_k\}$'s.

For special classes of serial sequence $\{s_k\}$ in an irreducible space $V[\Psi(x)]$ for an irreducible characteristic polynomial $\Psi(x)$ of degree $L$ whose period $\tau$ is relatively prime to $MN$, let a PSRG with the state transition matrix $T$, the initial state vector $d_0$ and the generating vectors $h_j$, $j=0, 1, \ldots, N-1$, be a minimal PSRG generating the $N$ sequences $U_{ij}, j=0, 1, \ldots, N-1$, where $U_i$ is the $i$th $MN$-decimated sequence of the serial sequence $\{s_k\}$.

Then the PSRG having the state transition matrix $T$, the initial state vector $d_0$ and the generating vectors $h_j$, $j=0, 1, \ldots, N-1$, such that

$$
\begin{align*}
\tilde{T} &= \\
\tilde{d}_0 &= \\
\tilde{h}_j &= \\
\end{align*}
$$

is an $(M, N)$ minimal PSRG for the serial sequence $\{s_k\}$, where $p$ is the smallest integer meeting the relation $pMN \equiv 1$.

The serial and the MPDSS's can be contrasted as depicted in Fig.1(a) and (b). In the $M$-bit parallel DSS, $N$ parallel input data bitstreams $\{b^j_k\}$, $j=0, 1, \ldots, N-1$, are scrambled before $M$-bit interleaved multiplexing by adding the parallel scrambling sequences $\{s^j_k\}$, $j=0, 1, \ldots, N-1$, and the scrambled bitstream $\{b_k + s_k\}$ is demultiplexed after $M$-bit interleave demultiplexing by adding the parallel descrambling sequences $\{s^j_k\}$, $j=0, 1, \ldots, N-1$. To make the scrambled bitstream $\{b_k + s_k\}$ in Fig.1(b) identical to the serial-descrambled bitstream $\{b_k + s_k\}$ in Fig.1(a) for the same parallel input data bitstreams $\{b^j_k\}$, the PSRGs should be organized to generate the parallel scrambling sequences $\{s^j_k\}$'s in (2), and the parallel sampling should be done in such a way that the samples $s^j_k$'s generated by the parallel sampling are identical to those generated by the serial sampling. In addition, the correction logic should also be changed such that the parallel descrambler is synchronized to the parallel scrambler at the final correction time. Note that the serial scrambling in Fig.1(a) is done at the transmission rate $f_t$, but the parallel scrambling in Fig.1(b) is done at the base rate $f_b$, which is an $N$th of the transmission rate $f_t$.

3. Parallel Shift Register Generators

We consider the $(M, N)$ PSRGs generating the parallel sequences in (2) for a scrambling sequence in an irreducible space, noting that a primitive space is an irreducible space. Then we obtain the following theorem which describes how to determine the state transition matrix, the initial state vector and the generating vectors of a minimal $(M, N)$ PSRG associated with an irreducible space.

**Theorem 1 (PSRG for MPDSS):** For a serial scrambling sequence $\{s_k\} = s^j_k \cdot \mathbf{E}_{\Psi_m(x)}$ in the irreducible space $V[\Psi(x)]$ of dimension $L$, let its period $\tau$ be relatively prime to $MN$. Then, for an $L \times L$ nonsingular matrix $R$ and its $ML \times L$ augmentation $R_M$ defined by

$$
\begin{align*}
\tilde{T} &= \\
\tilde{d}_0 &= \\
\tilde{h}_j &= \\
\end{align*}
$$

The $i$th $n$-decimated sequence $U_{ij}, i=0, 1, \ldots, n-1$, of a sequence $\{s_k\}$ refers to the sequence $\{s_{i+k}\}$. Refer to Ref.[3] for a more detailed description on this.

Refer to Refs.[3] and [7] for the convention of notation and the operation of the DSS and PDSS. Note that the MPDSS is a generalization of the PDSS in which parallelism is made multibit based.

All of non-zero sequences in an irreducible space $V[\Psi(x)]$ have the same period $\tau$, which is the smallest integer for which $\tau^2 + 1$ is a multiple of the irreducible characteristic polynomial $\Psi(x)$. For a more detailed description on this, refer to Ref.[9].
the PSRG with the state transition matrix $T$, the initial state vector $d_0$ and the generating vectors $h_j$ of the form

$$T = \begin{bmatrix} R \cdot A_{\psi(x)}^{t} & 0 & \mathbf{I}_{(M-1)L \times (M-1)L} \end{bmatrix}, \quad (6a)$$

$$d_0 = \bar{R}_M \cdot s,$$  

$$h_j = \begin{bmatrix} R^{j-1} \cdot A_{\psi(x)}^{t} \cdot e_0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \quad j = 0, 1, \ldots, N-1. \quad (6c)$$

is a minimal $(M, N)$ PSRG for the serial scrambling sequence $\{ s_k \}$. 

**Proof:** We prove the theorem using (3) and (4). Let $V[\psi_m(x)]$ be the minimal space for the $MN$-decimated sequences $U_i, i = 0, 1, \ldots, MN - 1$, of the serial scrambling sequence $\{ s_k \}$; and let $s_j, j = 0, 1, \ldots, N-1,$ be the initial vector of the $(jM)$th $MN$-decimated sequence $U_{jM}$. Then, $\psi_m(x)$ is a degree-$L$ factor of $x^{L-1} + 1$ whose extension $\psi_m(x^{MN})$ is a multiple of $\psi(x)$[5]; and the initial vector $s_j$ becomes $s_j = \left[ s_jM \right] s_jM+MN \ldots s_jM+(L-1)MN \right]^t = \left[ s^t \cdot A_{\psi(x)}^{t \cdot M} \cdot e_0 \right] (M-1)MN \cdot s \ldots \left( A_{\psi(x)}^{t \cdot (M-1)MN} \cdot s \right)^t \cdot \left( A_{\psi(x)}^{t \cdot (M-1)MN} \cdot e_0 \right)$. Since $\psi_m(x)$ is a degree-$L$ irreducible polynomial such that $\psi_m(x)$ divides $\psi_m(x^{MN})$, the minimal polynomial of $(A_{\psi(x)}^{t \cdot M})$ is $\psi_m(x)$. So the matrix $\left[ s \left( A_{\psi(x)}^{t \cdot (M-1)MN} \cdot s \right)^t \right.$ is nonsingular. Inserting $Q = R \cdot \left[ s \left( A_{\psi(x)}^{t \cdot (M-1)MN} \cdot s \right)^t \right.$ into (3), we can easily obtain the state transition matrix $T = R \cdot \left( A_{\psi(x)}^{t \cdot M} \right) \cdot R^{-1}$, the initial state vector $d_0 = R \cdot s$ and the generating vectors $h_j = \left( R^{j-1} \cdot A_{\psi(x)}^{t \cdot M} \cdot e_0 \right)$, $j = 0, 1, \ldots, N-1$, of a minimal PSRG generating the $(iM)$th $MN$-decimated sequences $U_{jM}, j = 0, 1, \ldots, N-1$. Inserting these parameters into (4), we obtain the minimal $(M, N)$ PSRG with the state transition matrix $T$ in (6a), the generating vectors $h_j$ in (6c), and the initial state vector $d_0 = \left[ R^t \left( R \cdot \left( A_{\psi(x)}^{t \cdot (M-1)MN} \right)^t \right) \right.$.

**Fig. 1** Block diagrams of (a) serial and (b) multibit-parallel DSSs.
Corollary 1 (PSRG for PDSS): For a serial scrambling sequence \( s_k = s^l \cdot E_{\Psi(x)} \) in the irreducible space \( V[\Psi(x)] \) of dimension \( L \), let its period \( \tau \) be relatively prime to \( N \) for the case \( M = 1 \). Then, for a nonsingular matrix \( R \), the PSRG with the state transition matrix \( T \), the initial state vector \( d_0 \) and the generating vectors \( h_j \)'s of the form

\[
T = R \cdot (A_{\Psi(x)}^{(l)})^N \cdot R^{-1},
\]

\[
d_0 = R \cdot s,
\]

\[
h_j = (R^t)^{-1} \cdot A_{\Psi(x)}^{(l)} \cdot e_0, j = 0, 1, \ldots, N - 1,
\]

is a minimal \((1, N)\) PSRG for the serial scrambling sequence \( s_k \).

Differently from the MPDSS case with \( M > 1 \), the initial state vector \( d_0 \) of a minimal \((1, N)\) PSRG for the PDSS can be arbitrarily chosen to be an \( L \)-vector.

4. Parallel Samplings

We now consider how to realize parallel samplings in the MPDSS. For parallel sampling, it is the most important to determine the parallel sampling times \( \hat{t}_i \)'s and the sampled sequence numbers \( l_i \)'s such that the samples taken by these parameters are identical to the samples taken by the original serial sampling. The following theorem describes how to determine these parameters.

Theorem 2A (Parallel Sampling for MPDSS): For a serial scrambling sequence \( s_k \), let \( s_k \), \( j = 0, 1, \ldots, N - 1 \), be the \( j \)th parallel sequence generated by an \((M, N)\) PSRG for \( s_k \). Then, a sample \( z \) taken from the serial scrambling sequence \( s_k \) at the sampling time \( \alpha \) corresponds to the sample taken from the \( l \)th parallel sequence \( s_{l_k} \) at the parallel sampling time \( \hat{\alpha} \), where \( l \) is the quotient of the integer \( r \) divided by \( M \) (i.e., \( r = lM + \hat{r} \)), and \( \hat{\alpha} \) is \( M \) times the integer \( q \) plus the remainder of the integer \( r \) divided by \( M \) (i.e., \( \alpha = qM + \hat{r} \)), where \( q \) and \( r \) are respectively the quotient and the remainder of \( \alpha \) divided by \( M \) (i.e., \( \alpha = qM + r \)).

Proof: Since the sample \( z \) is taken from the scrambling sequence \( s_k \) at the sampling time \( \alpha = qM + r \), we have the relation \( z = s_k = s_{qM + r} \). Therefore, by (2), \( z = s_{qM + r} \), that is, \( z \) is identical to the sample taken from the \( l \)th parallel sequence \( s_{l_k} \) at the sampling time \( \hat{\alpha} \).

To incorporate the concurrent parallel sampling [10] in the MPDSS, we need to change the sample transmission times as follows:

Theorem 2B (Parallel Sample Transmission for MPDSS): For a serial scrambling sequence \( s_k \), let \( s_k \), \( j = 0, 1, \ldots, N - 1 \), be the \( j \)th parallel sequence generated by an \((M, N)\) PSRG for \( s_k \). Then, a sample \( z \) transmitted over the serial-scrambled signal \( s_k \) at the sample transmission time \( \gamma \) is transmitted over the \( m \)th parallel sequence \( s_{l_k}^m \) at the parallel sample transmission time \( \hat{\gamma} \), where \( m \) is the quotient of the
integer \( r \) divided by \( M \) (i.e., \( r = mM + \hat{r} \)), and \( \hat{\gamma} \) is \( M \) times the integer \( q \) plus the remainder of the integer \( r \) divided by \( M \) (i.e., \( \hat{\gamma} = qM + \hat{r} \)), where \( q \) and \( r \) are respectively the quotient and the remainder of \( \gamma \) divided by \( MN \) (i.e., \( \gamma = qMN + r \)).

**Proof:** This theorem can be proved in a way similar to that of Theorem 2A.

For the concurrent parallel sampling, if we move the \( i \)-th parallel sampling time \( \alpha_i \) obtained by Theorem 2A to the \( i \)-th parallel sample transmission time \( \gamma_i \) obtained by Theorem 2B, we get, by (1), the sampling vector

\[
\mathbf{v}_i = (T^r)^{\alpha_i - \gamma_i} \mathbf{h}_{l_i},
\]

where \( T \) and \( h_i \)'s are respectively the state transition matrix and the generating vectors of an \((M, N)\) PSRG, and \( l_i \) is the sampled sequence number obtained by Theorem 2A.

**Example 2 (MPDSS Scrambler):** For the serial scrambling sequence \( \{ s_k \} \) in the scrambling space \( V[x^4 + x+1] \) whose sampling and sample transmission times are respectively \( \alpha_0 = 0, \alpha_1 = 3, \alpha_2 = 20, \alpha_3 = 23 \) and \( \gamma_0 = 0, \gamma_1 = 2, \gamma_2 = 20, \gamma_3 = 22 \), we realize an MPDSS scrambler with \( M = N = 2 \). By Theorem 2A, the parallel sampling times are \( \alpha_0 = 0, \alpha_1 = 1, \alpha_2 = 10, \alpha_3 = 11 \), and the sampled sequence numbers are \( l_0 = 0, l_1 = 1, l_2 = 0, l_3 = 1 \); and by Theorem 2B, the parallel sample transmission times are \( \gamma_0 = 0, \gamma_1 = 0, \gamma_2 = 10, \gamma_3 = 10 \), and the transmitted sequence numbers are \( m_0 = 0, m_1 = 1, m_2 = 2, m_3 = 1 \). If we employ the minimal (2, 2) PSRG in Fig. 2(a) and move the parallel sampling times \( \alpha_i \)'s to the parallel sample transmission times \( \gamma_i \)'s, then we obtain the sampling vectors \( \mathbf{v}_0 = \mathbf{v}_2 = \mathbf{e}_0 \) and \( \mathbf{v}_1 = \mathbf{v}_3 = \mathbf{e}_6 \) for this concurrent parallel sampling. The resulting MPDSS scrambler employing the concurrent parallel sampling is as shown in Fig. 3.

For the parallel sampling and the parallel sample transmission of the PDSS, we have the following two corollaries, which are obtained by setting \( M = 1 \) in Theorem 2, noting that \( \hat{r} = 0 \) for \( M = 1 \).

**Corollary 2A (Parallel Sampling for PDSS):** For a serial scrambling sequence \( \{ s_k \} \), let \( \{ s_k^i \} \), \( j = 0, 1, \cdots, N - 1 \), be the parallel sequence generated by a \((1, N)\) PSRG for \( \{ s_k \} \). Then, a sample \( z \) taken from the serial scrambling sequence \( \{ s_k \} \) at the sampling time \( \alpha \) corresponds to the sample taken from the \( l \)-th parallel sequence \( \{ s_k^l \} \) at the parallel sampling time \( \hat{\alpha} \), where \( l \) and \( \hat{\alpha} \) are respectively the remainder and the quotient of \( \alpha \) divided by \( N \) (i.e., \( \alpha = \hat{\alpha}N + l \)).

**Corollary 2B (Parallel Sample Transmission for PDSS):** For a serial scrambling sequence \( \{ s_k \} \), let \( \{ s_k^i \} \), \( j = 0, 1, \cdots, N - 1 \), be the parallel sequence generated by a \((1, N)\) PSRG for \( \{ s_k \} \). Then, a sample \( z \) transmitted over the serial-scrambled signal at the sample transmission time \( \gamma \) is transmitted over the \( m \)-th parallel-scrambled signal at the parallel sample transmission time \( \hat{\gamma} \), where \( m \) and \( \hat{\gamma} \) are respectively the remainder and the quotient of \( \gamma \) divided by \( N \) (i.e., \( \gamma = \hat{\gamma}N + m \)).

**5. Parallel Corrections**

Finally, we consider how to perform parallel corrections for a descrambler \((M, N)\) PSRG to achieve synchronization in the MPDSS. For this, we have to determine the parallel correction times \( \hat{\beta}_i \)'s and the parallel correction vectors \( \mathbf{c}_i \)'s for immediate correction [10]. We assume that the sample transmission times are uniformly distributed, and \( K \leq N \) samples are transmitted at a parallel sample transmission time. In this case, the sampling vectors at the sample transmission times are all identical, that is,

\[
\gamma_{iK} = \gamma_{iK+1} = \cdots = \gamma_{iK+K-1} = i\hat{\gamma},
\]

\[
i = 0, 1, \cdots, J - 1,
\]

\[
\hat{\mathbf{v}}_n = \hat{\mathbf{v}}_{K+n} = \cdots = \hat{\mathbf{v}}_{K(J-1)+n},
\]

\[
n = 0, 1, \cdots, K - 1,
\]

where \( \hat{\gamma} \) denotes the sample transmission interval. For convenience, we consider the case when \( K \) is a submultiple of the dimension \( L \) of the scrambling space \( V[\Psi(x)] \). Then, \( J = L/K \), which is an integer. We also assume for an efficient correction that the correction times are uniformly distributed, and the correction vectors are all identical, that is,

\[
\hat{\beta}_{iK} = \hat{\beta}_{iK+1} = \cdots = \hat{\beta}_{iK+K-1} = i\hat{\gamma} + \hat{\beta},
\]

\[
i = 0, 1, \cdots, J - 1,
\]

\[
\mathbf{c}_n = \mathbf{c}_{K+n} = \cdots = \mathbf{c}_{K(J-1)+n},
\]

\[
n = 0, 1, \cdots, K - 1,
\]

where \( \hat{\beta} \) denotes the correction delay. Then, the timing relation for this synchronization process is as depicted in Fig. 4. It is indicated in the figure that \( K \) samples are simultaneously taken at each sample transmission time \( i\hat{\gamma} \), and the related corrections are made \( \hat{\beta} \) time later.
As discussed in Sect. 3, the initial state vector \( \tilde{d}_0 \) of the descrambler \((M, N)\) PSRG is one of the 2\(^L\) ML-vectors obtained by inserting the 2\(^L\) values of \(s\) into (6b), that is, \( \tilde{d}_0 = \widetilde{R}_M \cdot s \), where \(s\) is an arbitrary \(L\)-vector. Thus, by (11b) and (12) we obtain the relation
\[
\delta_{(J-1)\gamma+\hat{\beta}} = \Lambda \cdot \tilde{R}_M \cdot (s + \Delta_{\alpha}^{-1} \cdot z).
\]
Therefore, to achieve synchronization in the MPDSS, we must choose the correction delay \(\hat{\beta}\) and the correction vectors \(\hat{c}_n\)'s such that the \(ML \times L\) matrix \(\Lambda \cdot \tilde{R}_M\) for the correction matrix \(\Lambda\) in (13) is a zero matrix. The following theorem describes how to choose the correction delay \(\hat{\beta}\) and the correction vectors \(\hat{c}_n\)'s to make \(\Lambda \cdot \tilde{R}_M\) zero.

**Theorem 3 (Parallel Correction for MPDSS):** For the descrambler \((M, N)\) PSRG with the state transition matrix \(T\) in (6a) and the generating vector \(h_j, j = 0, 1, \ldots, N-1\), in (6c), the \(ML \times L\) matrix \(\Lambda \cdot \tilde{R}_M\) for the correction matrix \(\Lambda\) in (13) and the relevant augmented matrix \(\tilde{R}_M\) in (5) becomes a zero matrix, if and only if the correction vectors \(\hat{c}_n, n = 0, 1, \ldots, K-1\), have the expression
\[
\hat{c}_n = T^{(J-1)\gamma+\hat{\beta}} \cdot \tilde{R}_M \cdot \Delta_{\alpha}^{-1} \cdot e_{(J-1)K+n}
\]
for an arbitrarily chosen correction delay \(\hat{\beta} \leq \gamma\).

**Proof:** We first establish the following lemma whose proof we omit for brevity.

**Lemma 2:** For \(n = 0, 1, \ldots, K-1\),
\[
\begin{align*}
\hat{v}_n^t \cdot T^{(J-1)\gamma+\hat{\beta}} \cdot \tilde{R}_M \cdot \Delta_{\alpha}^{-1} &= e_i^{(K+n)} \\
&= 0, 1, \ldots, J-1,
\end{align*}
\]
for the relevant augmented matrix \(\tilde{R}_M\), the sample vector \(z\), and the discrimination matrix \(\Delta_{\alpha}^{-1}\).

Since the synchronization in the MPDSS is achieved at the final correction time \((J-1)\gamma+\hat{\beta}\), for synchronization, the state distance vector \(\delta_{(J-1)\gamma+\hat{\beta}}\) should become zero regardless of the initial state distance vector \(\delta_0\) where \(\delta_0 \equiv \tilde{d}_0 + \tilde{d}_k\). The correction matrix \(\Lambda\) representing their relation such that
\[
\delta_{(J-1)\gamma+\hat{\beta}} = \Lambda \cdot \delta_0,
\]
can be determined by the following lemma, which can be proved in a way similar to the derivation of the correction matrix in Ref. [7].

**Lemma 1:** For the descrambler \((M, N)\) PSRG with the state transition matrix \(T\) in (6a) and the generating vector \(h_j, j = 0, 1, \ldots, N-1\), in (6c), the correction matrix \(\Lambda\) of the MPDSS is
\[
\Lambda = (T^t + \hat{c}_0 \cdot v_0^t \cdot T^{(J-1)\gamma+\hat{\beta}} + \hat{c}_1 \cdot v_1^t \cdot T^{(J-1)\gamma+\hat{\beta}} + \cdots + \hat{c}_{K-1} \cdot v_{K-1}^t \cdot T^{(J-1)\gamma+\hat{\beta}})^{(J-1)\gamma+\hat{\beta}} \cdot \widetilde{R}_M \cdot (T^{(J-1)\gamma+\hat{\beta}})^{(J-1)\gamma+\hat{\beta}} \cdot \Delta_{\alpha}^{-1} \cdot e_{(J-1)K+n}.
\]

\[\square\]
Fig. 5 An example of MPDSS descrambler employing the concurrent parallel sampling and the immediate correction.

equation for \(i = J - 1\). Now we assume that \(A \cdot \vec{R}_M \cdot \Delta_{\alpha}^{-1}, e_{(i-1)K+n} = 0, J = 1, J-2, \ldots, i\). Then, from (15c), we have the relation \(A \cdot \vec{R}_M \cdot \Delta_{\alpha}^{-1}, e_{(i-1)K+n} = (T^i + \hat{c}_0 \cdot \hat{v}_0^i \cdot \hat{T}_p^{i-\beta} + \cdots + \hat{c}_{K-1} \cdot \hat{v}_{K-1}^{i-\beta} \cdot T^{i-\beta})^{j-1}, (T^{i-1})^{j-\beta} \cdot \vec{R}_M \cdot \Delta_{\alpha}^{-1}, e_{(i-1)K+n} + \hat{c}_n\). Inserting (14) into this and applying (15b), we obtain \(A \cdot \vec{R}_M \cdot \Delta_{\alpha}^{-1}, e_{(i-1)K+n} = (T^i + \hat{c}_0 \cdot \hat{v}_0^i \cdot \hat{T}_p^{i-\beta} + \cdots + \hat{c}_{K-1} \cdot \hat{v}_{K-1}^{i-\beta} \cdot T^{i-\beta})^{j-1}, T^{i-1})^{j-\beta} \cdot \vec{R}_M \cdot \Delta_{\alpha}^{-1}, \sum_{j=1}^{J-1} \sum_{i=0}^{K-1} u_{j,i} \cdot \hat{c}_n \cdot e_{(i-1)K+n}\), which can be rewritten, by (15c), \(A \cdot \vec{R}_M \cdot \Delta_{\alpha}^{-1}, e_{(i-1)K+n} = \sum_{j=1}^{J-1} \sum_{i=0}^{K-1} u_{j,i} \cdot \hat{c}_n \cdot \hat{c}_n \cdot e_{(i-1)K+n} + \hat{c}_n\). But it is zero, since it was assumed that \(A \cdot \vec{R}_M \cdot \Delta_{\alpha}^{-1}, e_{(i-1)K+n} = 0, \hat{c}_n = \hat{c}_n + \hat{c}_n\). This completes the proof of the "if" part.

Next we prove the "only if" part. Inserting \(i = J - 1\) into (15c), we have the relation \(A \cdot \vec{R}_M \cdot \Delta_{\alpha}^{-1}, e_{(j-1)K+n} = T^{(J-1)}^{j-\beta} \cdot \vec{R}_M \cdot \Delta_{\alpha}^{-1}, e_{(j-1)K+n} + \hat{c}_n\). Therefore, if \(A \cdot \vec{R}_M = 0\), then \(\hat{c}_n = T^{(J-1)}^{j-\beta} \cdot \vec{R}_M \cdot \Delta_{\alpha}^{-1}, e_{(j-1)K+n}\). □

According to the theorem, the correction vectors \(\hat{c}_n\)'s in (14) make the \(ML \times L\) matrix \(A \cdot \vec{R}_M\) zero for arbitrarily chosen correction delay \(\beta\). Therefore, to realize an immediate correction, we can select the correction delay \(\beta = 1\), and then select the correction vectors \(\hat{c}_n\)'s using (14).

**Example 3 (MPDSS Descrambler):** For the serial scrambling sequence \(\{ s_k \}\) in the scrambling space \(V[x^2 + x + 1]\) whose sampling times and sample transmission times are respectively \(\alpha_0 = 0, \alpha_1 = 3, \alpha_2 = 20, \alpha_3 = 23\) and \(\gamma_0 = 0, \gamma_1 = 2, \gamma_2 = 20, \gamma_3 = 22\), we realize an MPDSS descrambler with \(M = 1\). In this case, the parallel sampling times, the sampled sequence numbers, the parallel sample transmission times and the transmitted sequence numbers are respectively \(\alpha_0 = 0, \alpha_1 = 10, \alpha_2 = 11, l_0 = 0, l_1 = 1, l_2 = 0, l_3 = 1, \gamma_0 = 0, \gamma_1 = 2, \gamma_2 = 10, \gamma_3 = 10, m_0 = 0, m_1 = 1, m_2 = 0, m_3 = 1\) (refer to Example 2). If we employ the minimal \((2, 2)\) PSRG in Fig. 2(b) and move the parallel sampling times \(\hat{c}_1\)'s to the parallel sample transmission times \(\hat{c}_1\)'s, then we obtain the sampling vectors \(v_0 = v_2 = e_0\) and \(v_1 = v_3 = e_4 + e_0\) for this concurrent parallel sampling. From the parallel sample transmission times \(\hat{c}_1\)'s, we observe that \(\hat{c}_1 = 10, K = 2\) and \(J = L/K = 2\). To realize the immediate correction, we insert the correction delay \(\beta = 1\) into (14) along with \(\hat{R} = [e_0 A_1^4, e_0 A_3^6, e_0 A_2^8, e_0 A_3^{12}]\). Then we obtain the correction vectors \(\hat{c}_0 = [01001000]^t\) and \(\hat{c}_1 = [10001111]^t\). The resulting MPDSS descrambler employing the concurrent sampling and the immediate correction is as shown in Fig. 5. This descrambler can be used in conjunction with the MPDSS scrambler in Fig. 3.

□

For the parallel correction of the PDSS, we have the following corollary, which is obtained by setting \(M = 1\) in Theorem 3, recalling the relation \(\vec{R}_1 = \vec{R}\).

**Corollary 3 (Parallel Correction for PDSS):** For the descrambler \((1, N)\) PSRG with the state transition matrix \(T\) in (7a) and the generating vector \(h_j, j = 0, 1, \ldots, N - 1\) in (7c), the \(L \times L\) matrix \(A \cdot \vec{R}\) for the correction matrix \(A\) in (13) and the relevant nonsingular matrix \(\vec{R}\) becomes a zero matrix, if and only if the correction vectors \(\hat{c}_n, n = 0, 1, \ldots, K - 1\), have the
expression

\[ \hat{c}_n = T^{(J-1)\hat{\gamma} + \hat{\beta}} \cdot R \cdot \Delta_n^{-1} \cdot e_{(J-1)K+n} \]

(16)

for an arbitrarily chosen correction delay \( \hat{\beta} \leq \hat{\gamma} \).

6. Conclusions

In this paper, we have considered the MPDSS techniques for use in the multibit-interleaved multiplexing environments. We have developed the techniques for realizing the PSRGs, the parallel sampling and the parallel correction circuits, which are the fundamental components for implementing the MPDSS scramblers and descramblers. The resulting three sets of theorems and the attached corollaries therefore provide the essential means for realizing the MPDSS and the PDSS.

In case the period of the serial scrambling sequence in an irreducible space is relatively prime to \( MN \) and \( N \) parallel sequences are interleaved \( M \)-bit based, we can obtain the state transition matrix \( T \) and the generating vectors \( h_i \)'s of a PSRG for the MPDSS by inserting an arbitrary nonsingular matrix \( R \) into (6a) and (6c) in Theorem 1 respectively. However, the initial state vector \( d_0 \) should be taken to be one of the \( 2^L \cdot ML \)-vectors obtained by inserting the \( 2^L \) possible values of the initial vector \( s \) into (6b).

In regard to parallel sampling in the MPDSS, the sampling vectors \( v_i \)'s for the concurrent sampling can be obtained by inserting the parallel sampling times \( \hat{\alpha}_i \)'s, the sampled sequence numbers \( \hat{\gamma}_i \), and the parallel sample transmission times \( \hat{\gamma}_i \)'s obtained by Theorems 2A and 2B into (8). As to parallel corrections in the MPDSS, we can set the correction delay \( \hat{\beta} = 1 \), and determine the correction vectors \( \hat{c}_i \)'s for uniformly distributed immediate correction according to (14) in Theorem 3.

The results summarized in Corollaries 1 to 3 for the PDSS are the special cases respectively of Theorems 1 to 3 for the MPDSS, which are obtained by setting \( M = 1 \) to the three theorems. Likewise, the results in Ref.[7] for the PDSS treat a special case of the PDSS corollaries in which two samples are simultaneously transmitted at each sample transmission time (i.e., \( K = 2 \)). Therefore, Theorems 1 to 3 can be viewed as the most general form of guidelines for parallel DSS realizations, and one can easily extend it as different sampling and sample transmission schemes arise.

References


Seok Chang Kim was born in Taegu, Korea, on August 16, 1964. He received the B.S., the M.E., and the Ph.D. degrees in electronics engineering from Seoul National University, Seoul Korea, in 1987, 1989, and 1994, respectively. Since September 1994 he has been with AT&T Bell Laboratories, Middletown, NJ, as a post-doctoral researcher. His research interests include digital transmission, digital communication, integrated broad-band networks, digital signal processing, and signal processing for telecommunication. Dr. Kim is a coauthor of Scrambling Techniques for Digital Transmission (Springer-Verlag, 1994), and holds three U.S. patents.
Byeong Gi Lee was born in Daecheon, Korea, on May 12, 1951. He received the B.S. and M.E. degrees in 1974 and 1978, respectively, from Seoul National University, Seoul, Korea, and Kyungpook National University, Taegu, Korea, both in electronics engineering, and the Ph.D. degree in 1982 from the University of California, Los Angeles, in electrical engineering. From 1974 to 1979 he was with the Department of Electronics Engineering of ROK Naval Academy, Chinhae, Korea, as an instructor and naval officer in active service. From 1982 to 1984 he worked for Granger Associates, Santa Clara, CA, as a senior engineer doing research and development on applications of digital signal processing to digital transmission. During the period 1984 to 1986 he worked for AT&T Bell Laboratories, North Andover, MA, as a member of the technical staff participating in lightwave transmission system development along with related standard works. Since September 1986 he has been with the Department of Electronics Engineering, Seoul National University. His current fields of interest include theory and applications of digital signal processing, digital transmission and integrated broad-band networks, and circuit theory. He is a coauthor of Introduction to ISDN. Broadband Telecommunication Systems, Electronics Engineering Experiment Series (4 volumes), and the editor of HDTV Dictionary, all in Korean; and a coauthor of Broadband Telecommunication Technology (Artech House, 1993) and Scrambling Techniques for Digital Transmission (Springer-Verlag, 1994) in English. He holds six U.S. patents with one more pending. He received the 1984 Myril B. Reed Best Paper Award from the Midwest Symposium on Circuits and Systems, and exceptional contribution awards from AT&T Bell Laboratories. He is a member of KITE, KICS, KISS, and ASK; a senior member of IEEE; and a member of Sigma Xi.