Applications of Sequence Space and SRG Theories to Distributed Sample Scrambling

Seok Chang Kim and Byeong Gi Lee, Fellow, IEEE

Abstract—In this paper, we consider how to apply the sequence space and the shift register generator (SRG) theories to distributed sample scrambling (DSS), which exhibits the best performance in scrambling of small frame-sized signals. We first consider how to predict scrambling sequences using their samples, which is a basic problem for a proper synchronization within the DSS systems. Then for DSS scramblers, we consider how to determine the scrambler SRG’s and the sampling times for conveying information on the scrambling sequence; and for DSS descramblers, we consider how to determine the descrambler SRG’s, the correction times, and the correction vectors for a proper synchronization. We further examine how to realize the scramblers and the descramblers with minimized circuit complexity. Finally, we demonstrate how to apply the results to DSS scramblers and descramblers for application in cell-based asynchronous transfer mode (ATM) transmission.

Index Terms—Correction times, correction vectors, distributed sample scrambling, sampling times, sequence space, shift register generator.

I. INTRODUCTION

DISTRIBUTED sample scrambling (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 [1]. Differently from the self-synchronous scrambling (SSS) [2], the DSS generates the SRG sequence independently of the user data; and differently from the frame synchronous scrambling (FSS) [3], the DSS continues scrambling without periodically resetting the SRG states. Therefore, the DSS exhibits the most efficient scrambling effect for small frame-sized signals among the three scrambling techniques. The DSS technique has been adopted in the cell-based asynchronous transfer mode (ATM) transmission within the BISDN, recently standardized by ITU-T [4].

The structure of the DSS is as shown in Fig. 1, and its operation is as follows. For scrambling and descrambling, an SRG-generated sequence is added to the corresponding input streams, respectively, in the scrambler and the descrambler, as for the case of the FSS. For synchronization, some samples of the scrambler SRG sequence are taken by the sampling function, and are conveyed to the descrambler in parallel with the scrambled bit stream. The descrambler compares them with its own generated samples, and if the two samples are different, it initiates a correction logic to change the descrambler SRG state such that the descrambler SRG can eventually get synchronized to the scrambler SRG.

For the synchronization of DSS, two fundamental conditions are necessary—the sample time condition that describes when to take samples from scrambling sequences, and the correction time and vector condition that describe when and how to correct the descrambler SRG state for synchronization [1]. The synchronization conditions provided in [1] are derived based on the assumption that the SRG’s in the scrambler and descrambler pair are identical to each other. However, according to the sequence space and the SRG theories recently developed in [5], an SRG sequence can be generated by different types of SRG’s. This means that different types of SRG’s may be used for the scrambler and descrambler within the same DSS system as long as they meet the relevant synchronization conditions. This testifies that the sequence space and the SRG theories can add a new dimension of insight to the design of the DSS.

Therefore, in this paper, we will examine the behaviors of the DSS in view of the sequence space and the SRG theories, and consider how to apply the theories in developing efficient synchronization arrangements. Further, we will discuss how to minimize the circuit complexity of the scrambler and the descrambler, and how to eliminate additional timing circuitry for generating the sampling times and the correction times.

The paper is organized as follows. We first consider how to predict the scrambling sequences using their samples in Section II. Then we consider how to efficiently realize the DSS scramblers and the DSS descramblers, respectively, in Sections III and IV. Next, we discuss how to eliminate additional timing circuitry in the scrambler and the descrambler in Section V, and finally, in Section VI, we demonstrate how to apply the results to the ATM-cell scrambling in the BISDN.

II. PREDICTION OF SCRAMBLING SEQUENCES

Based on the sequence space and the SRG theories described in [5] we examine the behaviors of scrambling sequences generated by SRG’s, and consider how to predict the scrambling sequences using their samples.\(^1\)

For an SRG with length \(L\) and state transition matrix \(T\), we define by the generating vector \(h\) an \(L\) vector representing the

\(^1\)Refer to [5] for the definition of the terminology and the proofs of various relations that are taken from the sequence space and the SRG theories.
relation between the scrambling sequence \( \{ s_k \} \) and the SRG sequence vector \( D \) or, more specifically,

\[
\{ s_k \} = h^* \cdot D,
\]

and define by the *scrambling space* \( V[T,h] \) the set whose elements are the scrambling sequences \( \{ s_k \} \)'s obtained by varying the initial state vectors \( d_0 \)'s or, more specifically,

\[
V[T,h] = \{ \{ s_k \} : s_k = h^* \cdot D \text{ for all initial state vectors } d_0 \}'s \}.
\]

Then, the scrambling space \( V[T,h] \) is determined by the following property.

**Property 1:** For an SRG with state transition matrix \( T \) and generating vector \( h \), the scrambling space \( V[T,h] \) is the sequence space \( V[\Psi_{T,a}(x)] \) whose characteristic polynomial \( \Psi_{T,a}(x) \) is the lowest degree polynomial meeting the relation

\[
h^* \cdot \Psi_{T,a}(T) = 0.
\]

**Proof:** We first prove that \( V[T,h] \subseteq V[\Psi_{T,a}(x)] \). Let \( \Psi_{T,a}(x) = \sum_{i=0}^{L-1} \psi_i x^i \), and let \( \{ s_k \} \) be the scrambling sequence in \( V[T,h] \) for an initial state vector \( d_0 \). Then, it suffices to show that \( \{ s_k \} \subseteq V[\Psi_{T,a}(x)] \). By (1), \( s_k = h^* \cdot d_k, k = 0,1,\ldots \), and hence we obtain the relation \( \sum_{i=0}^{L-1} \psi_i s_{k+i} = \sum_{i=0}^{L-1} \psi_i h^* \cdot T^i \cdot d_k = h^* \cdot \Psi_{T,a}(T) \cdot d_k \). But this is 0 due to (3). Therefore, \( \{ s_k \} \subseteq V[\Psi_{T,a}(x)] \).

To complete the proof, we now prove that \( V[\Psi_{T,a}(x)] \subseteq V[T,h] \). Let \( \{ s_k \} = s^i \cdot E_{\Psi_{T,a}(x)}(x) \) for an initial vector \( s \). Then, it suffices to show that \( \{ s_k \} \subseteq V[T,h] \), which is equivalent to showing that there exists an initial state vector \( d_0 \) that makes the scrambling sequence \( \{ s_k \} \) identical to \( \{ s_k \} \). Since \( \Psi_{T,a}(x) \) is the lowest degree polynomial meeting (3), the \( L \) vectors \( h^* \cdot T^i \cdot s, i = 0,1,\ldots,L-1 \), are linearly independent. Therefore, we can choose an initial state vector \( d_0 \) such that \( h^* \cdot T^i \cdot d_0 = c^i \cdot s \) for \( i = 0,1,\ldots,L-1 \), and for this initial state vector \( d_0 \), the scrambling sequence \( \{ s_k \} \) has the initial vector \( s \). Therefore, the scrambling sequence \( \{ s_k \} \) is identical to \( \{ s_k \} = s^i \cdot E_{\Psi_{T,a}(x)}(x) \) since \( \{ s_k \} \) is an element of the sequence space \( V[\Psi_{T,a}(x)] \). This completes the proof.

The property describes how to determine the scrambling space \( V[T,h] \). That is, the scrambling space \( V[T,h] \) is identical to the sequence space \( V[\Psi_{T,a}(x)] \) whose characteristic polynomial \( \Psi_{T,a}(x) \) is the lowest degree polynomial meeting (3). Therefore, any scrambling sequence \( \{ s_k \} \) generated by an SRG with the state transition matrix \( T \) and the generating vector \( h \) belongs, regardless of its initial state vector \( d_0 \), to the sequence space \( V[\Psi_{T,a}(x)] \) whose characteristic polynomial \( \Psi_{T,a}(x) \) is the lowest degree polynomial meeting (3).

For an SRG with the state transition matrix \( T \), we consider how to determine the largest dimensional scrambling space of all scrambling spaces \( V[T,h] \)'s obtained by varying the generating vectors \( h \)'s, which we call the *scrambling maximal space*.

**Property 2:** For an SRG, its scrambling maximal space is identical to its SRG maximal space.

**Proof:** For an SRG with the state transition matrix \( T \), let \( V[T] \) and \( \hat{V}[T] \) denote the SRG maximal space and the scrambling maximal space. We first prove that \( \hat{V}[T] \subseteq V[T] \). For this, we consider the scrambling space \( V[T,h] \) for a generating vector \( h \). If \( \{ s_k \} \subseteq V[T,h] \), by the definition of scrambling space, there exists an initial state vector \( d_0 \) whose scrambling sequence is identical to the sequence \( \{ s_k \} \), and hence by the definition of SRG space, the SRG space \( V[T,d_0] \) for this initial state vector \( d_0 \) includes the sequence \( \{ s_k \} \). That is, \( \{ s_k \} \subseteq V[T,d_0] \), and so \( \{ s_k \} \subseteq V[T] \) since an SRG space is a subspace of the SRG maximal space. Therefore, \( V[T,h] \subseteq V[T] \). Noting that this relation holds for an arbitrary generating vector \( h \), we have the relation \( \hat{V}[T] \subseteq V[T] \).

In a similar manner, we can prove that \( V[T] \subseteq \hat{V}[T] \), and so we have the property.

Therefore, we can state that for an SRG with the state transition matrix \( T \), the scrambling maximal space \( \hat{V}[T] \), the SRG maximal space \( V[T] \), and the sequence space \( V[\Psi(x)] \) for the minimal polynomial \( \Psi(x) \) of \( T \) are all identical. On the other hand, according to the definition of the basic SRG (BSRG), a BSRG for a sequence space \( V[\Psi(x)] \) is an SRG of the smallest length whose SRG maximal space is identical to the sequence space \( V[\Psi(x)] \). So, combining this with Property 2, we obtain the following property.

**Property 3:** An SRG of the smallest length whose scrambling maximal space is identical to the sequence space \( V[\Psi(x)] \) is a BSRG for the sequence space \( V[\Psi(x)] \).

For such a BSRG, we consider how to choose a generating vector \( h \) for which the scrambling space \( V[T,h] \) becomes the sequence space \( V[\Psi(x)] \). By Property 2, the scrambling maximal space is identical to the SRG maximal space \( V[T] \), which becomes \( V[\Psi(x)] \) in this BSRG case. Therefore, the generating vector \( h \) should be chosen such that the scrambling
space \( V[T, \mathbf{h}] \) is identical to the scrambling maximal space \( V[T] = V[\Psi(x)] \). We call such a generating vector a maximal generating vector. The maximal generating vector for a BSRG can be determined by the following property.

**Property 4:** A generating vector \( \mathbf{h} \) is a maximal generating vector of the BSRG for a sequence space \( V[\Psi(x)] \) of dimension \( L \), if and only if the discrimination matrix \( \Delta_{T, \mathbf{h}} \) defined by

\[
\Delta_{T, \mathbf{h}} \equiv \begin{bmatrix}
\mathbf{h}^t \\
\mathbf{h}^t \cdot T \\
\vdots \\
\mathbf{h}^t \cdot T^{L-1}
\end{bmatrix}
\]  

is nonsingular for the state transition matrix \( T \) taken similar to the companion matrix \( A_{\Psi(x)} \).

**Proof:** We first prove the “if” part of the property. Let \( \mathbf{h} \) be a generating vector that makes \( \Delta_{T, \mathbf{h}} \) nonsingular. Then, the \( L \) vectors \( \mathbf{h}^t \cdot T^i \), \( i = 0, 1, \ldots, L-1 \), are linearly independent. Therefore, the degree of the lowest degree polynomial \( \Psi_{T, \mathbf{h}}(x) \) that meets (3) is \( L \) or higher, and so by Property 1, the dimension of the scrambling space \( V[T, \mathbf{h}] \) is \( L \) or higher. However, since the dimension of the scrambling maximal space \( V[T] = V[\Psi(x)] \) is \( L \), it should be the scrambling maximal space \( V[T] \). That is, \( \mathbf{h} \) is a maximal generating vector.

Next, we prove the “only if” part by contradiction. Suppose that there exists a generating vector \( \mathbf{h} \) such that \( \Delta_{T, \mathbf{h}} \) is singular. Then, the \( L \) vectors \( \mathbf{h}^t \cdot T^i \), \( i = 0, 1, \ldots, L-1 \), are linearly dependent. Therefore, the degree of the lowest degree of polynomial \( \Psi_{T, \mathbf{h}}(x) \) that meets (3) is less than \( L \), and so by Property 1, the dimension of the scrambling space \( V[T, \mathbf{h}] \) is less than \( L \). However, this is a contradiction to the assumption that \( \mathbf{h} \) is a maximal generating vector.

Combining this property with Property 3, we can state that if an SRG is a smallest length SRG whose scrambling space is the sequence space \( V[\Psi(x)] \), its state transition matrix \( T \) is similar to the companion matrix \( A_{\Psi(x)} \), and its generating vector \( \mathbf{h} \) makes the discrimination matrix \( \Delta_{T, \mathbf{h}} \) in (4) nonsingular.

So far, we have considered the scrambling space and the scrambling maximal space formed by scrambling sequences. On this basis, we now consider how to predict the scrambling sequence from their samples, assuming that the scrambling space is known.

We consider the scrambling sequence \( \{s_k\} \) generated by an SRG whose scrambling space is the sequence space \( V[\Psi(x)] \) of dimension \( L \). Since the scrambling sequence \( \{s_k\} \) is an element of the scrambling space \( V[\Psi(x)] \), it can be completely determined if its initial state vector \( s \) is known. Since the initial vector \( s \) of the scrambling sequence \( \{s_k\} \) is an \( L \) vector, it is necessary for a valid prediction to be furnished with a minimum of \( L \) samples of \( \{s_k\} \).

For a sequence space \( V[\Psi(x)] \) with the characteristic polynomial \( \Psi(x) = \sum_{i=0}^{L-1} v_i x^i \), the companion matrix is defined to be

\[
A_{\Psi(x)} = \begin{bmatrix}
0 & 1 & 0 & \cdots & 0 \\
\vdots & & & & \vdots \\
0 & 0 & \cdots & & 1 \\
\end{bmatrix},
\]

for the \( (L - 1) \)-row vector \( \mathbf{e}_L = \begin{bmatrix} 1 & 0 & \cdots & 0 \end{bmatrix} \), the \( (L - 1) \)-column vector \( \mathbf{v} = [v_1, v_2, \cdots, v_{L-1}] \), and the \( (L - 1) \)-column vector \( \mathbf{i} = [v_1, v_2, \cdots, v_{L-1}] \).

Suppose that the \( L \) samples \( s_i, i = 0, 1, \ldots, L-1 \), are taken from the scrambling sequence \( \{s_i\} \) at the \( i \)th sampling time \( \alpha_i, i = 0, 1, \ldots, L-1 \), respectively, such that \( s_i = \alpha_i \) and let the sample vector \( z \) denote the \( L \) vector formed by the \( L \) samples \( z_i \), i.e., \( z = [z_0, z_1, \cdots, z_{L-1}] \). Then, since \( z = s \cdot A_{\Psi(x)} \cdot \mathbf{e}_L \), by a fundamental relation in the sequence space theory \([5]\),

\[
z = \Delta_{\alpha} \cdot s
\]

where \( \Delta_{\alpha} \) is the \( L \times L \) discrimination matrix defined by

\[
\Delta_{\alpha} \equiv \begin{bmatrix}
\mathbf{e}_L^t \cdot (A_{\Psi(x)} \cdot \mathbf{e}_L)^{\alpha_0} \\
\mathbf{e}_L^t \cdot (A_{\Psi(x)} \cdot \mathbf{e}_L)^{\alpha_1} \\
\vdots \\
\mathbf{e}_L^t \cdot (A_{\Psi(x)} \cdot \mathbf{e}_L)^{\alpha_{L-1}}
\end{bmatrix}.
\]

Therefore, the initial vector \( s \) can be determined as follows.

**Property 5:** For a scrambling sequence \( \{s_k\} \) generated by an SRG whose scrambling space is the sequence space \( V[\Psi(x)] \) of dimension \( L \), the initial vector \( s \) of the scrambling sequence \( \{s_i\} \) can be determined from the sample vector \( z \) formed by the samples taken at the sampling times \( \alpha_i, i = 0, 1, \ldots, L-1 \), by inverting (5) (i.e., \( s = \Delta_{\alpha}^{-1} \cdot z \)), if and only if the sampling times \( \alpha_i \)’s are chosen such that the discrimination matrix \( \Delta_{\alpha} \) in (6) is nonsingular.

Therefore, to predict the scrambling sequence \( \{s_k\} \) from its samples, the sampling times \( \alpha_i \)’s should be chosen such that the corresponding discrimination matrix \( \Delta_{\alpha} \) is nonsingular. We call such sampling times predictable sampling times. Note that \( \Delta_{\alpha} \) in (6) depends only on the scrambling space \( V[\Psi(x)] \) and the sampling times \( \alpha_i \)’s, regardless of the state transition matrix \( T \) and the generating vector \( \mathbf{h} \) of SRG.

### III. Scramblers for DSS

We consider how to choose the state transition matrix \( T \) and the generating vector \( \mathbf{h} \) for a DSS scrambler, and how to decide the sampling times \( \alpha_i \)’s when taking samples from the scrambling sequence \( \{s_k\} \).

In the DSS, a PRBS is used for scrambling as in the case of the FSS. However, differently from the FSS, the scrambling sequence \( \{s_k\} \) in the DSS varies depending on the initial state vector \( \mathbf{d}_0 \) of the scrambler SRG. According to the definition of scrambling space, the scrambling sequence \( \{s_k\} \) is an element of the scrambling space \( V[\Psi(x)] \) and according to \([7]\), a nonzero sequence \( \{s_k\} \) in a primitive (sequence) space \( V[\Psi_p(x)] \) for a primitive polynomial \( \Psi_p(x) \) is a PRBS. Therefore, any nonzero scrambling sequence \( \{s_k\} \) generated by an SRG whose scrambling space is a primitive space \( V[\Psi_p(x)] \) becomes a PRBS. In other words, the scrambler SRG in the DSS always renders a primitive scrambling space. The following theorem describes how to choose the state transition matrix \( T \) and the generating vector \( \mathbf{h} \) of scrambler SRG whose scrambling space becomes a primitive space \( V[\Psi_p(x)] \).

\[\text{Note that } \mathbf{e}_L \text{ denotes the basis vector whose } i\text{th element is 1 and the others are 0, for } i = 0, 1, \cdots, L-1.\]
**Theorem 1 (Scrambler SRG):** A matrix \( \mathbf{T} \) is the state transition matrix of the smallest-length SRG whose scrambling maximal space is the primitive space \( V[\psi_P(x)] \), if and only if it is similar to the companion matrix \( A_{\psi_P(x)} \) and a generating vector \( \mathbf{h} \) is a maximal generating vector for the SRG with the state transition matrix \( \mathbf{T} \) similar to \( A_{\psi_P(x)} \), if and only if it is a nonzero vector.

Proof: The first part of the theorem is directly obtained by Property 3 since the state transition matrix \( \mathbf{T} \) of a BSRG for the primitive space \( V[\psi_P(x)] \) is similar to \( A_{\psi_P(x)} \) and the second part can be easily proved by noting that a scrambling space \( V[\mathbf{T}, \mathbf{h}] \) is a subspace of the scrambling maximal space \( V[\mathbf{T}] = V[\psi_P(x)] \) and a primitive polynomial is an irreducible polynomial.

Therefore, for the DSS scrambler employing the primitive scrambling space \( V[\psi_P(x)] \), its state transition matrix \( \mathbf{T} \) should be chosen to be similar to \( A_{\psi_P(x)} \) but its generating vector \( \mathbf{h} \) can be chosen to be an arbitrary nonzero vector.

We now consider the sampling times \( \alpha_i \)'s of the scrambling sequence \( \{s_k\} \). In the DSS, since the scrambling sequence \( \{s_k\} \) used in scrambling is predicted by its samples \( z_i \)'s, the sampling times \( \alpha_i \)'s of the samples \( z_i \)'s should be predictable sampling times. Therefore, we obtain the following theorem directly from Property 5.

**Theorem 2 (Sampling Times):** For a scrambling sequence \( \{s_k\} \) whose scrambling space is the sequence space \( V[\psi(x)] \) of dimension \( L \), let \( \alpha_i, i = 0, 1, \ldots, L - 1 \), be the sampling times of the \( i \)-th sample \( z_i \) of the sample vector \( z \). Then, if the sampling times \( \alpha_i \)'s are chosen such that the discrimination matrix \( \Delta_\alpha \) in (6) is nonsingular, the scrambling sequence \( \{s_k\} \) determined by the relation

\[
\{s_k\} = (\Delta_\alpha^{-1} \cdot z)^T \cdot E_{\psi(x)} \tag{7}
\]

for the elementary sequence vector \( E_{\psi(x)} \); otherwise, it is impossible to determine the scrambling sequence \( \{s_k\} \).

The theorem means that the scrambling sequence \( \{s_k\} \) is predicted by (7) only if the sampling times \( \alpha_i \)'s are predictable. Therefore, what is important for the DSS scrambler is to take the sampling times \( \alpha_i \)'s such that the discrimination matrix \( \Delta_\alpha \) in (6) becomes nonsingular. Once this requirement is met, the descrambler can generate the scrambler SRG sequence \( \{s_k\} \) by employing the relation in (7).

**IV. DESCRAMBLERS FOR DSS**

Assuming that the sampling times \( \alpha_i \)'s are taken to be predictable, we consider how to choose the state transition matrix \( \mathbf{T} \) and the generating vector \( \mathbf{h} \) of a descrambler SRG, and further, how to choose the correction times \( \beta_i \)'s and the correction vectors \( \mathbf{c}_i \)'s to generate the predicted scrambling sequences. Among many possible choices of the descrambler SRG’s, we consider the smallest length descrambler SRG which can be synchronized to the scrambling sequence \( \{s_k\} \).

With regard to the descrambler SRG structure, we get the following theorem directly from Property 3.

4One of the fundamental properties of the sequence space \( V[\psi(x)] \) is that its elementary sequence vector \( E_{\psi(x)} \) can be inner-producted with the initial vector \( \mathbf{s} \) to produce the sequence \( \{s_k\} \), i.e., \( \{s_k\} = \mathbf{s}^T \cdot E_{\psi(x)} \).

**Theorem 3 (Descrambler SRG):** For a scrambling sequence \( \{s_k\} \) whose scrambling space is the sequence space \( V[\psi(x)] \), let \( \mathbf{T} \) and \( \mathbf{h} \) be, respectively, the state transition matrix and the generating vector of the smallest length synchronizable descrambler SRG. Then, \( \mathbf{T} \) is similar to the companion matrix \( A_{\psi(x)} \), and \( \mathbf{h} \) is a maximal generating vector.

Therefore, in order to synchronize a descrambler SRG to a scrambling sequence \( \{s_k\} \) in the scrambling space \( V[\psi(x)] \), the state transition matrix \( \mathbf{T} \) should be chosen to be similar to \( A_{\psi_P(x)} \) and the generating vector \( \mathbf{h} \) should be maximal. Note that this is a weak requirement that does not require \( \mathbf{T} \) and \( \mathbf{h} \) to be identical, respectively, to \( \mathbf{T} \) and \( \mathbf{h} \) of the corresponding scrambler.

With regard to the correction times \( \beta_i \)'s and the correction vectors \( \mathbf{c}_i \)'s, the following theorem provides the guidelines.

**Theorem 4 (Correction Times and Correction Vectors):** Let \( \mathbf{T} \) and \( \mathbf{h} \) be, respectively, the state transition matrix and the generating vector of the smallest length descrambler SRG synchronizable to the scrambling sequence \( \{s_k\} \) whose scrambling space is the \( L \)-dimensional sequence space \( V[\psi(x)] \). Then, this descrambler is synchronized to the scrambling sequence \( \{s_k\} \), and if only if the correction vectors \( \mathbf{c}_i \)'s have, for the correction time \( \beta_i \)'s, the expressions

\[
\mathbf{c}_i = \begin{cases} 
\Delta_{\mathbf{T}, \mathbf{h}}^{-1} \cdot (A_{\psi_P(x)}^t)^{\beta_i} \cdot \Delta_{\alpha}^{-1} \cdot \left( e_i + \sum_{j=0}^{\beta_i} u_{ij} e_j \right), & i = 0, 1, \ldots, L - 2 \\
\Delta_{\mathbf{T}, \mathbf{h}}^{-1} \cdot (A_{\psi_P(x)}^t)^{\beta_i} \cdot \Delta_{\alpha}^{-1} \cdot e_{L-1}, & i = L - 1 
\end{cases}
\tag{8}
\]

where \( u_{ij} \) is either 0 or 1 for \( i = 0, 1, \ldots, L - 2 \) and \( j = i + 1, i + 2, \ldots, L - 1 \).

Proof: To prove the theorem, we first establish the following two equations:

\[
\mathbf{T} = \Delta_{\mathbf{T}, \mathbf{h}}^{-1} \cdot A_{\psi_P(x)}^t \cdot \Delta_{\mathbf{T}, \mathbf{h}} \tag{9}
\]

\[
A = (\mathbf{T}^t)^{\alpha_0} \cdot \mathbf{h} \cdot (\mathbf{T}^t)^{\alpha_1} \cdot \mathbf{h} \cdots (\mathbf{T}^t)^{\alpha_{L-1}} \cdot \mathbf{h}^t = \Delta_{\alpha} \cdot \Delta_{\mathbf{T}, \mathbf{h}} \tag{10}
\]

To prove (9), we consider the matrix \( A_{\psi_P(x)}^t \cdot \Delta_{\mathbf{T}, \mathbf{h}} \) for \( \psi(x) = \sum_{i=0}^{L} \psi \cdot x^i \). Then, by (4) and the definition of the companion matrix \( A_{\psi_P(x)}^t \), we get \( A_{\psi_P(x)}^t \cdot \Delta_{\mathbf{T}, \mathbf{h}} = \Delta_{\alpha} \cdot \Delta_{\mathbf{T}, \mathbf{h}} \).

This yields (9) since \( \Delta_{\mathbf{T}, \mathbf{h}} \) is nonsingular for the maximal generating vector \( \mathbf{h} \). Equation (10) can be obtained by applying the relations \( \mathbf{T} = \Delta_{\mathbf{T}, \mathbf{h}}^{-1} \cdot A_{\psi_P(x)}^t \cdot \Delta_{\mathbf{T}, \mathbf{h}} \) and \( \mathbf{h}^t \cdot \Delta_{\mathbf{T}, \mathbf{h}}^{-1} = e_i \).

We assume that the scrambler SRG is identical to the descrambler SRG, that is, the state transition matrix and the generating vector of the scrambler SRG are \( \mathbf{T} \) and \( \mathbf{h} \) respectively. Note that this assumption is valid since the scrambling space \( V[\mathbf{T}, \mathbf{h}] \) becomes \( V[\psi(x)] \) due to Theorem
Then, by \( (10) \), \( \Delta \) is nonsingular, and hence by \([1, \text{eq. (18)}]\), the correction vectors \( \mathbf{c}_i \)'s become

\[
\mathbf{c}_i = \begin{cases} 
\hat{T}^{\Delta_{i-1}} \cdot \Delta_{i-1}^{-1} \cdot \left( \mathbf{e}_i + \sum_{j=i+1}^{L-1} u_{i,j} \mathbf{e}_j \right), & i = 0, 1, \ldots, L - 2 \\
\hat{T}^{\Delta_{L-1}} \cdot \Delta_{L-1}^{-1} \cdot \mathbf{e}_{L-1}, & i = L - 1.
\end{cases}
\]

Therefore, by \( (9) \) and \( (10) \), we have the correction vectors \( \mathbf{c}_i \)'s in \( (8) \).

According to theorem, the correction times \( \beta_i \)'s may be chosen arbitrarily, but the correction vectors \( \mathbf{c}_i \)'s should be chosen according to the expression in \( (8) \). Combining this theorem with Theorem 3, we can efficiently determine \( \hat{T}, \hat{h}, \beta_i \)'s, and \( \mathbf{c}_i \)'s of the smallest length descramblers as described in the following theorem.

**Theorem 5 (Realization of Descramblers):** For the scrambling sequence \( \{s_k\} \) whose scrambling space is the sequence space \( V[\Psi(x)] \) of dimension \( L \), let the sampling times \( \alpha_i, i = 0, 1, \ldots, L - 1 \), be predictable sampling times. Then, for a nonsingular matrix \( \hat{R} \), the descrambler with the state transition matrix \( \hat{T} \), the generating vector \( \hat{h} \), and the correction vectors \( \mathbf{c}_i \)'s of the form

\[
\hat{T} = R^{-1} \cdot A_{\Psi(x)}^0 \cdot R \\
\hat{h} = R^t \cdot e_0 \\
\mathbf{c}_i = \begin{cases} 
R^{-1} \cdot (A_{\Psi(x)}^0)^{i} \cdot \Delta_{i-1}^{-1} \cdot \left( \mathbf{e}_i + \sum_{j=i+1}^{L-1} u_{i,j} \mathbf{e}_j \right), & i = 0, 1, \ldots, L - 2 \\
R^{-1} \cdot (A_{\Psi(x)}^0)^{L-1} \cdot \Delta_{L-1}^{-1} \cdot \mathbf{e}_{L-1}. & i = L - 1
\end{cases}
\]

for the correction times \( \beta_i \)'s and arbitrary binary parameters \( u_{i,j} \)'s is a smallest length synchronizable descrambler.

Proof: The state transition matrix \( \hat{T} \) in \( (11a) \) is similar to \( A_{\Psi(x)}^0 \), so it meets Theorem 3. Inserting \( (11a) \) and \( (11b) \) into \( (4) \), and applying the relations \( e_0^t \cdot (A_{\Psi(x)}^0)^{i} \cdot e_i = 0, 1, \ldots, L - 1 \), we obtain \( \Delta_{\hat{T}, \hat{h}} = \hat{R} \) which is nonsingular. Therefore, \( \hat{h} \) in \( (11b) \) is a maximal generating vector, which meets Theorem 3. Inserting \( \Delta_{\hat{T}, \hat{h}} = \hat{R} \) into \( (8) \), we get the correction vectors \( \mathbf{c}_i \)'s in \( (11c) \). 

V. DSS WITH MINIMIZED TIMING CIRCUITY

In the DSS, timing circuits are necessary to generate clocks for the sampling and correction times. Moreover, additional timing circuits are needed to generate the clocks that indicate when the samples are actually transmitted. We call the time \( \gamma_i, i = 0, 1, \ldots, L - 1 \), at which the sample \( z_k \) is transmitted, the \( i \)th sample transmission time. If samples are transmitted at the moment they are sampled, the sampling time itself becomes the sample transmission time. But, in general, the sample transmission time is decided depending on the available slots in the frame format, so in practice, it is impossible to change the sample transmission times arbitrarily. Consequently, timing circuitry is required to generate various kinds of clocks for the relevant storing and retrieval of samples, and such a timing circuit is usually complex. Therefore, in this section, we consider how to minimize the complexity of the related timing circuit.

A. Concurrent Sampling

Since the available slots for sample transmission are not changeable, we rather consider changing the sampling times to be identical to the sample transmission times. Then, additional timing circuitry for the generation of the sampling times will not be necessary because other timing circuits that readily exist to generate clocks for frame formatting can be utilized for this. However, this does not always work because the sampling times fitted to the available transmission slots may not be the predictable sampling times. Therefore, it does not provide a complete solution.

To completely solve the timing circuitry problem, we need to allow for independence between the sampling time and the sample transmission time, but instead, take the samples at the transmission times, yet keeping the effect of sampling at the desired predictable sampling times. We call this concurrent sampling as the sampling occurs concurrently with the sample insertion for transmission, which can be achieved by adopting the concept of a sampling vector introduced in [6]. According to this, the sampling vector \( \psi \) is a vector describing the relation of the sample \( z \) to the corresponding state vector \( d_{\gamma_i} \), i.e., \( z = \psi^t \cdot d_{\gamma_i} \), and the sample \( z \) taken at the sampling time \( \alpha \) using the sampling vector \( \psi \) is identical to the sample taken at the sampling time \( \gamma_i \) using the sampling vector \( \psi = (T^t)^{\alpha-\gamma_i} \cdot \psi \). Therefore, in the DSS, the sample \( z_{\gamma_i} \) to be sampled at sample time \( \alpha \) can be identified obtained at the sample transmission time \( \gamma_i \) if the sampling vector is switched to

\[
\psi = (T^t)^{\alpha-\gamma_i} \cdot \hat{h}
\]

since the original sampling vector used to be the generating vector \( \hat{h} \).

B. Immediate Correction

Differently from the case of the sampling times, we know from Theorem 4 that the correction times can be chosen arbitrarily. Therefore, we can arrange them to come immediately after the sampling times, thus eliminating the additional timing circuit needed to generate the correction times. We call such a correction scheme an immediate correction.

If we combine the immediate correction with the concurrent sampling, we can design descramblers that do not require any
Fig. 3. DSS scrambler for scrambling of the cell-based ATM transmission signal.

additional circuitry for the sampling time and correction time generation, or for the relevant sample storing and retrieval. In this arrangement, we can move the sampling times $\gamma_i$'s to the sample transmission times $\beta_i$'s at the cost of the sampling vector generating circuit, and we can choose the correction times $\beta_i$'s to be $\beta_i = \gamma_i + 1$ at no additional cost.

VI. APPLICATIONS TO ATM CELL SCRAMBLING

Now, we consider how to apply the results we have derived so far for an efficient design of DSS's to use in the cell-based ATM transmission environment.

A. Scrambling of Cell-Based ATM Signals

According to the ITU-T document [4], in the scrambling of the cell-based ATM signal, the DSS employs the scrambling sequence $\{s_k\}$ in the primitive scrambling space $V[x^{31} + x^3 + 1]$ of dimension $L = 31$. The 31 samples $s_0$ through $s_{30}$ taken from the scrambling sequence $\{s_k\}$ are conveyed to the descrambler over the header error control (HEC) field in the ATM cell header in unit of two samples per ATM cell, as illustrated in Fig. 2. This implies that the $i$th sample transmission times $\gamma_i$'s are

$$\gamma_{2i} = 424i, \quad i = 0, 1, \ldots, 15$$
$$\gamma_{2i+1} = 424i + 1, \quad i = 0, 1, \ldots, 14$$

(13)

since the ATM cell is composed of 53 bytes or 424 bits. The sampling times $\alpha_i$'s of the samples $z_i$'s are supposed to be uniformly distributed, i.e.,

$$\alpha_i = 212i - 211, \quad i = 0, 1, \ldots, 30$$

(14)

Comparing the sampling transmission times $\gamma_i$'s and the sampling times $\alpha_i$'s, we find that the sample transmission time and the sampling time for an even-indexed sample $z_{2i}$, $i = 0, 1, \ldots, 15$, do not coincide, while those for an odd-indexed sample $z_{2i+1}$, $i = 0, 1, \ldots, 14$, do. That is, each even-indexed sample is transmitted after being stored for 211 bit times. In Fig. 2, the sample $s_{211}$ indicates such an even-indexed sample which is transmitted at the sample transmission time $\beta_i$, but is taken at the sampling time $\gamma_i$. Therefore, if the scrambler SRG is chosen as the SSSD with the state transition matrix $T = A_{2^{31} + 2^{3} + 1}^T$ and the generating vector $h = a_0 + a_3$, the scrambler for distributed-sample scrambling of the cell-based ATM transmission signal can be drawn as in Fig. 3. In the figure, we observe that two kinds of timing signals are required—one for generating the sample transmission times $\gamma_i$'s in (13), and the other for generating the sampling times $\alpha_i$'s in (14).

In order to check if the sampling times $\alpha_i$'s in (14) are predictable, we insert these and $\gamma_i$ into (6). Then, we obtain the discrimination matrix $\Delta_{\alpha}$, which is nonsingular. Therefore, the sampling times $\alpha_i$'s in (14) are predictable, so the DSS is synchronizable.

For the correction of the scrambler SRG, the correction times $\beta_i$'s are supposed to be uniformly spaced such that

$$\beta_i = 212i + 1, \quad i = 0, 1, \ldots, 30$$

(15)

If we choose the nonsingular matrix

$$R = [(a_0 + a_3) \quad A_{z^{31} + z^3 + 1} \cdot (a_0 + a_3) \quad \cdots \quad A_{z^{31} + z^3 + 1} \cdot (a_0 + a_3)]$$

(16)
then by (11) we obtain the descrambler with the state transition matrix

\[
\begin{align*}
\hat{T} & = A_{x^{21}, x^{23}+1}^t \\
\hat{h} & = \gamma_0 + \gamma_3 \\
\gamma_0 & = \gamma_1 = \cdots = \gamma_{20} = \gamma_{21} = \gamma_3 + \gamma_{23} + \gamma_{24} + \gamma_{28},
\end{align*}
\]

Using these parameters, we can obtain the descrambler in Fig. 4. In this descrambler, three different timing signals are required for generating the sample transmission times in (13), the sampling times in (14), and the correction times in (15), as indicated in the figure.

**B. Equivalent DSS with Minimized Timing Circuitry**

As discussed in the previous section, an equivalent DSS can be obtained by employing the concurrent sampling and the immediate correction, and the resulting DSS has a minimized timing circuitry because the timing circuits for generating the sampling times and the correction times are all eliminated.

If we choose the scrambler SRG with the state transition matrix \( T = A_{x^{21}, x^{23}+1}^t \) and the generating vector \( h = \gamma_0 + \gamma_3 + \gamma_{21} \), and move the sampling times \( \alpha_i \)'s in (14) to the sampling transmission times \( \gamma_i \)'s in (13), then by (12), we obtain the sampling vectors \( \hat{v}_0 = \hat{v}_2 = \cdots = \hat{v}_{20} = A_{x^{21}, x^{23}+1}^t \cdot \hat{h} = \gamma_0 + \gamma_3 \) and \( \hat{v}_1 = \hat{v}_3 = \cdots = \hat{v}_{20} = h = \gamma_0 + \gamma_3 + \gamma_{21} + \gamma_{23} + \gamma_{24} + \gamma_{28}. \)

Then, inserting the nonsingular matrix \( R \) whose \( i \)th column is

\[
\begin{align*}
\begin{cases}
(A_{x^{21}, x^{23}+1}^{i+1})^{-1} \cdot (e_1 + e_8 + e_{11} + e_{18} + e_{22} + e_{23}), \\
(i = 0, 1, \cdots, 15) \\
(A_{x^{21}, x^{23}+1}^{i+1})^{-1} \cdot (e_0 + e_6 + e_{10} + e_{16} + e_{20}) \\
(i = 3, 4, \cdots, 7) \\
(A_{x^{21}, x^{23}+1}^{i+1})^{-1} \cdot (e_{23} + e_{24} + e_{30}) \\
(i = 8, 9, \cdots, 16) \\
(A_{x^{21}, x^{23}+1}^{i+1})^{-1} \cdot (e_1 + e_3 + e_{11} + e_{18} + e_{22} + e_{23}) \\
(i = 17, 18, \cdots, 30)
\end{cases}
\end{align*}
\]

Then, inserting the nonsingular matrix \( R \) whose \( i \)th column is

\[
\begin{align*}
\begin{cases}
(A_{x^{21}, x^{23}+1}^{i+1})^{-1} \cdot (e_1 + e_8 + e_{11} + e_{18} + e_{22} + e_{23}), \\
(i = 0, 1, \cdots, 15) \\
(A_{x^{21}, x^{23}+1}^{i+1})^{-1} \cdot (e_0 + e_6 + e_{10} + e_{16} + e_{20}) \\
(i = 3, 4, \cdots, 7) \\
(A_{x^{21}, x^{23}+1}^{i+1})^{-1} \cdot (e_{23} + e_{24} + e_{30}) \\
(i = 8, 9, \cdots, 16) \\
(A_{x^{21}, x^{23}+1}^{i+1})^{-1} \cdot (e_1 + e_3 + e_{11} + e_{18} + e_{22} + e_{23}) \\
(i = 17, 18, \cdots, 30)
\end{cases}
\end{align*}
\]
Fig. 5. Equivalent DSS scrambler employing the concurrent sampling.

For a proper synchronization within the DSS systems, it is fundamental to be able to predict the scrambling sequence from the conveyed samples. As a means to seek the answer, we introduced the concept of the scrambling space, and investigated various properties of the scrambling sequence based on the scrambling space concept. As a consequence, we reached the conclusion that the sampling times should be chosen such that the relevant discrimination matrix becomes nonsingular. For such predictable sampling times, the initial vector of the objected scrambling sequence can be predicted by the equation

\[
 s = A^{-1} \cdot z_c.
\]

In the DSS, a PRBS is used for scrambling as in the case of FSS, so the scrambling space renders a primitive space. Therefore, according to Theorem 1, the state transition matrix \( \mathbf{T} \) of the DSS scrambler should be chosen to be similar to the companion matrix \( A_d(z_c) \), but its generating vector \( \mathbf{h} \) can be chosen among any nonzero vectors. The scrambling sequence in the DSS can be determined from the samples through Theorem 2 if the sampling times are taken to be predictable, and cannot be determined otherwise.

Aside from the state transition matrix \( \mathbf{T} \) the generating vector \( \mathbf{h} \), and the sampling times \( \gamma_c \)'s, the correction vectors \( \mathbf{c}_r \)'s and the correction times \( \beta_c \)'s are additionally required for the DSS descrambler. According to Theorem 3, \( \mathbf{T} \) and \( \mathbf{h} \) of the descrambler are not necessarily the same as \( \mathbf{T} \) and \( \mathbf{h} \) for the scrambler as long as \( \mathbf{T} \) is similar to \( \mathbf{T} \) and \( \mathbf{h} \) is maximal. In contrast to the selection of sampling times, there is no restriction on the selection of correction times, and the related correction vectors are determined through Theorem 4.

In practical design of a DSS descrambler, the three core parameters \( \mathbf{T}, \mathbf{h}, \) and \( \mathbf{c}_r \)'s can be determined by inserting an arbitrary nonsingular matrix \( \mathbf{R} \) to the equations listed in Theorem 5. For an efficient descrambler design, however, repeated trials are necessary for an optimal choice of the matrix \( \mathbf{R} \) itself.

For an efficient DSS design, it is crucial to minimize the complexity of the timing circuits. Since the sample trans-
mission times are basically necessary for the actual sample transmission, it is desirable to be able to eliminate the circuits for the sampling and the correction time generation. This desire is completely satisfied by adopting the concept of concurrent sampling and immediate correction. That is, we move the sampling times to the sample transmission times, yet keeping the effect of sampling at the original sampling times (concurrent sampling), and for this, we adopt the concept of a sampling vector introduced in [6] to ensure the predictability of the new sampling times. Likewise, we move the correction times to the positions immediately following the sample transmission times (immediate correction), which can be done without any additional arrangement due to the arbitrariness of the correction times.

The applications of the sequence space and the SRG theories, therefore, have added a new dimension to the design of the DSS system by setting it free to take the state transition matrix and the generating vector for the descrambler differently from those for the scrambler, and by making it free to move the sampling and correction times to any desired positions. The design freedom thus obtained enables us to design DSS scramblers and descramblers in very efficient ways, which is well demonstrated in the ITU-T recommended DSS system design for cell-based ATM transmission. As a practical outcome of this work, we can now use the scrambler and the descrambler, respectively, in Figs. 5 and 6 instead of those, respectively, in Figs. 3 and 4, with the timing circuits for the generation of sampling pulses and the correction pulses completely eliminated.

REFERENCES


Seok Chang Kim was born in Taegu, Korea, on August 16, 1964. He received the B.S., M.E., and Ph.D. degree in electronics engineering from Seoul National University, Korea, in 1987, 1989, and 1994, respectively.

Since September 1994, he has been with Lucent Technologies 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 telecommunications. Dr. Kim is a coauthor of Scrambling Techniques for Digital Transmission (New York: Springer-Verlag, 1994), and holds three U.S. patents.
Byeong Gi Lee (S’80–M’82–SM’89–F’97) received the B.S. and M.E. degrees in electronics engineering respectively from Seoul National University and Kyungpook National University in Korea, and the Ph.D. degree in electrical engineering from the University of California at Los Angeles (UCLA).

He was with Electronics Engineering Department of ROK Naval Academy as an instructor and naval officer in active service from 1974 to 1979. He worked for Granger Associates, Santa Clara, CA, from 1982 to 1984 as a senior engineer responsible for applications of digital signal processing to digital transmission, and for AT&T Bell Laboratories, North Andover, MA, from 1984 to 1986 as a member of technical staff responsible for lightwave transmission system development along with related standard works. He joined the faculty of School of Electrical Engineering, Seoul National University in 1986, where he is now a professor. He is an Associate Editor of IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY and the Editor of IEEE Global Communications Newsletter. He is the vice chair of Asia Pacific Committee of IEEE ComSoc and the past chair of IEEE Communications Chapter of Seoul. His current fields of interest include signal processing, communication systems, and integrated telecommunication networks. He is a coauthor of Broadband Telecommunication Technology, 2nd ed., (Artech House, 1996), and Scrambling Techniques for Digital Transmission (Springer Verlag, 1994). He holds six U.S. patents with one more patent pending.

Dr. Lee 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 KICS, KITE, KISS, ASK, and Sigma Xi.