IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 1 June 2022, accepted 14 June 2022, date of publication 21 June 2022, date of current version 27 June 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3185066

Blind Estimation of Self-Synchronous Scrambler Using Orthogonal Complement Space in DSSS Systems

YOONJI KIM[1], (Member, IEEE), JUNGMIN KIM[2], (Member, IEEE), JUNGHWAN SONG[2], (Member, IEEE), AND DONGWEON YOON[1], (Senior Member, IEEE)
[1]Department of Electronic Engineering, Hanyang University, Seoul 04763, South Korea
[2]Department of Mathematics, Research Institute for Natural Sciences, Hanyang University, Seoul 04763, South Korea

Corresponding author: Dongweon Yoon (dwyoon@hanyang.ac.kr)

ABSTRACT In a non-cooperative context, a receiver has to estimate the communication parameters without any prior knowledge of the transmitter, which is highly demanding. Estimating a self-synchronous scrambler is even more challenging because the scrambling sequence of the self-synchronous scrambler is affected by the input sequence. This paper proposes an improved algorithm for blind estimation of a self-synchronous scrambler using the orthogonal property without any bias condition of the received signals in direct sequence spread spectrum (DSSS) systems. We first examine the linear relation of a scrambling sequence using the repetitive property of the spreading code used in a DSSS system. Using the obtained linear relation and the basis of the orthogonal complement space, we then acquire the feedback polynomial candidates of the scrambler. Finally, by calculating the greatest common divisor polynomial of the feedback polynomial candidates, we estimate the correct feedback polynomial. Through computer simulations, we verify that the proposed method achieves superior estimation performance compared to the existing method. Furthermore, we show that the proposed method has practically acceptable computational complexity. For these reasons, it is expected that the proposed method can be applied to blind estimation of a self-synchronous scrambler in a practical non-cooperative system.

INDEX TERMS Estimation, communication forensic, self-synchronous scrambler, linear feedback shift register.

I. INTRODUCTION

In non-cooperative contexts, such as spectrum surveillance and cognitive radio, a receiver has to blindly estimate the parameters used in a transmitter without prior knowledge of the transmitter in order to recover the information. In this regard, many studies have been conducted on blind estimation of communication parameters, such as modulation type [1], [2], source coding [3], channel coding [4]–[6], interleaving [7], line coding [8], etc.

The direct sequence spread spectrum (DSSS) system is widely used in military and commercial communication systems because of its low probability of intercept (LPI) and the robustness to the narrow-band interference [11]. In the DSSS system, a scrambler can be used as a randomizer by adding the scrambling sequence generated from a linear feedback shift register (LFSR) to the input of the scrambler. There are two major types of scramblers: the synchronous scrambler, which generates a scrambling sequence independently of the input bits, and the self-synchronous scrambler, whose input bits affect the state of the LFSRs.

Pertaining to the blind estimation of the scramblers, algorithms that utilize the bias of the received sequence were proposed in [10] and [11]. Moreover, estimation methods without using the bias condition of the received sequence were provided in [12]–[18]. References [12] and [13] presented the estimation methods that use the dual words of the channel code, and the rank-based estimation method was also provided in [14]. In particular, the estimation methods for the synchronous scrambler in DSSS systems were developed in [15] and [16], which employ a triple correlation and eigenvalue decomposition, respectively. However, the aforementioned methods suffer from high computational complexity due to the full search of all possible feedback

The associate editor coordinating the review of this manuscript and approving it for publication was Mohammad Alshabi.

polynomials [10]–[15] or huge matrix computation [16]. On the other hand, [17] most recently presented a method that blindly estimates the feedback polynomial of the synchronous scrambler in DSSS systems by using the repetitive property of the spreading code and the inherent linearity of the scrambled sequence. Compared to previous studies, the method in [17] showed remarkable estimation performance improvement and drastically reduced the computational complexity. As an extension of [17], [18] first presented a blind self-synchronous scrambler estimation method in the DSSS system. However, the method in [18] obtains only one feedback polynomial from Gaussian elimination, which can be wrong if the received signals suffer from severe noise. Therefore, it is encouraged to find more than one feedback polynomial candidate and verify them to improve estimation performance.

To solve the problem in [18], this paper proposes an improved algorithm for blind estimation of a self-synchronous scrambler using an orthogonal complement space without any bias condition of the received signals in DSSS systems. To achieve this, we first examine the linear relation of a scrambling sequence through the repetitive property of the spreading code used in the DSSS system. Using the obtained linear relation and the basis of the orthogonal complement space, we then acquire as many candidates for the feedback polynomial of the scrambler as possible. Considering the bit errors induced from a noisy channel, we conduct a verification process for each feedback polynomial candidate. Finally, we estimate the correct feedback polynomial by calculating the greatest common divisor (GCD) polynomial of all verified feedback polynomial candidates. To validate the proposed method, we carry out computer simulations and compare the estimation probabilities of the proposed method with the method in [18] for various degrees of feedback polynomials.

The contributions of this paper can be summarized as follows:

- The main contribution of this paper is that an improved self-synchronous scrambler estimation algorithm compared to the existing algorithm in [18] is developed. The specific contributions are described in what follows.
    - It is shown that the coefficient vectors of the multiples of the correct feedback polynomial form the basis of an orthogonal complement space spanned by the shift-and-added sequence of the received sequence.
    - A method of obtaining as many candidates as possible for the feedback polynomial of the self-synchronous scrambler is proposed, which utilizes the basis of the orthogonal complement space.
    - An effective process for the verification of each feedback polynomial candidate is provided by using the orthogonality of the coefficient vectors of the feedback polynomial candidate
    - An improved estimation algorithm that includes the methods of obtaining and verifying the feedback polynomial candidates is provided.

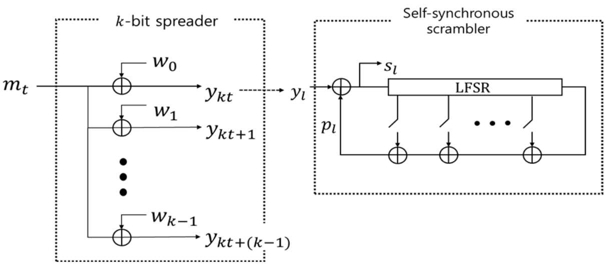

FIGURE 1. Simplified block diagram of a DSSS system with a self-synchronous scrambler.

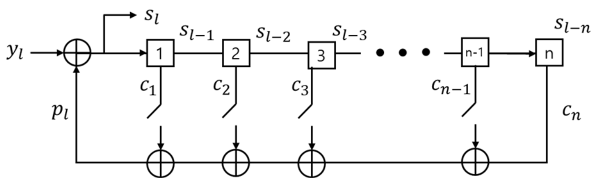

FIGURE 2. Self-synchronous scrambler for the feedback polynomial $c(x) = 1 + c_1x + c_2x^2 + \cdots + c_nx^n$.

The remainder of this paper is organized as follows. Section II describes the system model. Section IIU proposes a blind self-synchronous scrambler estimation algorithm. Section OV shows the estimation performance under various simulation setups and the execution time of the proposed algorithm, and Section V concludes the paper.

II. SYSTEM MODEL

Fig. 1 shows a simplified block diagram of a DSSS system with a self-synchronous scrambler, where m_t is a message bit, w_j is a spreading code bit, y_l is an input bit to the self-synchronous scrambler, p_l is a scrambling bit, and s_l is a scrambled bit. The spreader generates the spread sequence bit $(y_l)_{l=kt}^{l=kt+k-1}$ from the message bit m_t and the k-bit length spreading code $\left(w_j\right)_{j=0}^{j=k-1}$, which can be expressed as

$$y_{kt+j} = m_t \oplus w_j, \quad \text{for } 0 \leq j \leq k-1. \tag{1}$$

The scrambled bit s_l is then generated by adding the scrambling sequence bit p_l to the spread sequence bit y_l and can be expressed as

$$\begin{aligned} s_l &= y_l \oplus p_l \\ &= m_t \oplus w_j \oplus p_l, \text{for } l = kt + j. \end{aligned} \tag{2}$$

In Fig. 2, we depict a self-synchronous scrambler for the n degree feedback polynomial $c(x) = 1 + c_1x + c_2x^2 + \cdots + c_nx^n$. Then, the scrambling sequence $(p_l)_{l\geq 1}$, which is generated by the LFSR, has the following linear relation:

$$p_l = \oplus_{i=1}^{n} c_i s_{l-i}. \tag{3}$$

From (2) and (3), we obtain

$$s_l = y_l \oplus \left(\oplus_{i=1}^{n} c_i s_{l-i}\right), \text{ for } l \geq n. \tag{4}$$

Note that to estimate the feedback polynomial of the self-synchronous scrambler, it is necessary to remove the spread sequence bits $(y_l)_{l=kt}^{l=kt+k-1}$ from (4). Therefore, to cancel out the spread sequence bits in (4), u_l is defined as [18]

$$u_l = s_l \oplus s_{l+1} \oplus s_{l+k} \oplus s_{l+(k+1)}. \tag{5}$$

By substituting (2) to (5) and using the repetitive property of the spreading code, it can be readily seen that

$$u_l = p_l \oplus p_{l+1} \oplus p_{l+k} \oplus p_{l+k+1}, \quad \text{for } l \not\equiv 0 \mod k. \tag{6}$$

Then, by substituting (3) to (6), u_l can be rewritten as

$$u_l = \left(\oplus_{i=1}^{n} c_i u_{l-i}\right), \text{ for } l \not\equiv 0 \mod k,\ l \geq n. \tag{7}$$

III. PROPOSED ALGORITHM FOR ESTIMATION OF A SELF-SYNCHRONOUS SCRAMBLER

In this section, we propose an improved blind estimation method of a self-synchronous scrambler. First, we present an algorithm for the estimation of the self-synchronous scrambler in a noiseless channel and then extend it to a noisy channel.

A. BLIND ESTIMATION OF A SELF-SYNCHRONOUS SCRAMBLER IN A NOISELESS CHANNEL

For the self-synchronous scrambler estimation, we propose a method to acquire as many feedback polynomial candidates of the scrambler as possible by finding the basis of the orthogonal complement space. To do this, we first examine the orthogonality of the feedback polynomial coefficient vector.

With the vector representation, (7) can be expressed as follows:

$$\langle (1, c_1, \cdots, c_n), (u_l, u_{l-1}, \cdots, u_{l-n}) \rangle \mod 2 = 0, \quad \text{for } l \not\equiv 0 \bmod k, \tag{8}$$

where $\langle \cdot, \cdot \rangle$ represents the inner product. Let the vector $(1, c_1, \ldots, c_n)$ with the coefficients of the feedback polynomial of the self-synchronous scrambler be simplified to $\boldsymbol{c}$. According to (8), if $l \not\equiv 0 \bmod k$, then $\boldsymbol{c}$ is orthogonal to the consecutive n-length vectors of the sequence $(u_l, u_{l-1}, \cdots, u_{l-n})$ for $l \not\equiv 0 \bmod k$.

Now, we define the q-bit length vector $\boldsymbol{c}^{\gg j}$ as

$$\boldsymbol{c}^{\gg j} = \left(\overbrace{0, \cdots, 0}^{j}, 1, c_1.c_2. \cdots, c_n, \overbrace{0, \cdots, 0}^{q-j-n-1} \right), \quad j = 0, \ldots, q-n-1. \tag{9}$$

Then, from (8), we obtain

$$\left\langle (u_l)_{l=i}^{i-(q-1)}, \boldsymbol{c}^{\gg j} \right\rangle \mod 2 = 0, \quad \text{for } i \not\equiv 0 \bmod k. \tag{10}$$

From (10), we can see that the vectors $\boldsymbol{c}^{\gg j}$ are orthogonal to the consecutive q-bit length sequence $(u_l)_{l=i}^{i-(q-1)}$. Therefore, the vectors $\left\{\boldsymbol{c}^{\gg j} \middle| j = 0, \cdots, q-n-1\right\}$ belong to the orthogonal complement space of the vector space spanned by $(u_l)_{l=i}^{i-(q-1)}$. Note that $\left\{\boldsymbol{c}^{\gg j} \middle| j = 0, \cdots, q-n-1\right\}$ are the basis of the orthogonal complement space spanned by $(u_l)_{l=i}^{i-(q-1)}$ since each vector of $\boldsymbol{c}^{\gg j}$ is independent.

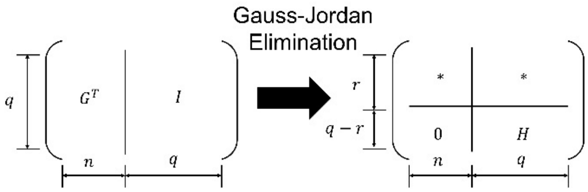

FIGURE 3. Finding the basis of the orthogonal complement space by using Gauss-Jordan elimination.

Therefore, finding the basis of the orthogonal complement space is equivalent to finding the candidates for the feedback polynomial of the self-synchronized scrambler. The basis of the orthogonal complement space can be obtained by using Gauss-Jordan elimination as shown in Fig. 3, which is based on Theorem 1 in [19]. For a matrix or a vector $\boldsymbol{A}$, we denote the transpose of $\boldsymbol{A}$ as $\boldsymbol{A}^T$.

Theorem 1 [19]: Let the matrix $\boldsymbol{A} = \left(\boldsymbol{G}^T \| \boldsymbol{I}\right)$ be the augmented matrix of the $q \times n$ matrix $\boldsymbol{G}^T$ with rank r and the $q \times q$ identity matrix $\boldsymbol{I}$. In addition, let $\boldsymbol{H}$ be the submatrix of size $(q-r) \times q$ at the lower right corner of the reduced row echelon form (RREF) of $\boldsymbol{A}$. Then, $\boldsymbol{H} \cdot \boldsymbol{G}^T = \boldsymbol{0}$ holds.

The algorithm finding the basis of the orthogonal complement space based on Theorem 1 is summarized in Algorithm 1. Since finding the orthogonal complement space is equivalent to finding the candidates of the feedback polynomial, which are indeed the multiples of $c(x)$, the feedback polynomial candidates can be obtained by using Algorithm 1.

Algorithm 1 Finding the Basis of the Orthogonal Complement Space

```
Input:
    n vectors of length q, $(v_i)_{i=1}^{q}$
Output:
    Basis of the orthogonal complement space
1.  Construct matrix $\boldsymbol{G} = \left(\boldsymbol{v}_1^T \middle| \boldsymbol{v}_2^T \middle| \cdots \middle| \boldsymbol{v}_n^T\right)$.
2.  Do binary Gauss-Jordan elimination on the
     augmented matrix $\boldsymbol{G} \| \boldsymbol{I}$.
3.  Return the row vectors of matrix $\boldsymbol{H}$ of $\boldsymbol{G} \| \boldsymbol{I}$.
```

Then, the feedback polynomial candidate that has the smallest degree is chosen as the feedback polynomial of the self-synchronous scrambler. We summarize the proposed blind estimation method of the feedback polynomial for a noiseless channel in Algorithm 2.

B. BLIND ESTIMATION OF A SELF-SYNCHRONOUS SCRAMBLER IN A NOISY CHANNEL

In this subsection, we extend Algorithm 2 to a noisy channel. In a noisy channel, a polynomial that is not a multiple of $c(x)$ can appear in the outputs of Algorithm 1 due to the bit

Algorithm 2 Blind Estimation of the Feedback Polynomial of the Self-Synchronous Scrambler in a Noiseless Channel

```
Input:
  $(s_l)_{l\geq 1}$ : scrambled sequence of length $S$
  $k$: spreading code length
  $n_{th}$: upper bound of the degree of the feedback
        polynomial
Output:
  $\theta$: Feedback polynomial
1.    $\Theta \leftarrow \emptyset$.
2.    $u_l \leftarrow s_l \oplus s_{l+1} \oplus s_{l+k} \oplus s_{l+(k+1)}$.
3.    For $j = 1$ to $n_{th}$
4.        $\boldsymbol{v}_j = (u_l)_{l=n_{th}+kj}^{n_{th}+kj-(n_{th}-1)}$
5.    Do Algorithm 1 with $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \cdots, \boldsymbol{v}_{n_{th}}\}$
6.    Add the result of Step 5 to $\Theta$.
7.    $\theta \leftarrow$ the feedback polynomial candidate that has
      the smallest degree in $\Theta$.
8.    Return $\theta$.
```

In Step 6, the output of Step 5 is converted into a polynomial and added to Θ.

Algorithm 3 Blind Estimation of the Feedback Polynomial of the Self-Synchronous Scrambler in a Noisy Channel

```
Input:
  $(s_l)_{l=1}^{S}$ : scrambled sequence of length $S$
  $k$: spreading code length
  $n_{th}$: upper bound of the degree of the feedback
        polynomial
  $L$: number of iterations, $h$: shift parameter
  $TH$: threshold for the verification
  $R$: verification parameter
Output:
  $\theta$: Feedback polynomial
1.    $\Theta \leftarrow \emptyset$.
2.    $u_l \leftarrow s_l \oplus s_{l+1} \oplus s_{l+k} \oplus s_{l+(k+1)}$.
3.    $offset \leftarrow n_{th}$
4.    For $ITER$=1 to $L$
5.        For $j = 1$ to $n_{th}$
6.            $\boldsymbol{v}_j = (u_l)_{l=offset+kj}^{offset+kj-(n_{th}-1)}$
7.        Do Algorithm 1 with $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \cdots, \boldsymbol{v}_{n_{th}}\}$
8.        $offset \leftarrow offset + k$
9.        Add the result of Step 7 to $\Theta$
10.   For each polynomial $\theta$ in $\Theta$,
11.       $\phi \leftarrow \deg(\theta) + 1$, $score_j \leftarrow 0$.
12.       For $j = 0$ to $n_{th} - \phi$
13.       $score_j = R^{-1} \sum_{t=1}^{R} \left[1 - \left\langle (u_l)_{l=n_{th}+kt}^{n_{th}+kt-(n_{th}-1)}, \theta^{\gg j} \right\rangle \bmod 2 = 0\right]$.
14.       If there is no $j$ such that $score_j < TH$, then
           delete $\theta$ from $\Theta$.
15.   $\theta \leftarrow$the GCD polynomial of all polynomials in $\Theta$
      using the Euclidean algorithm [20], [21].
16.   Return $\theta$.
```

The parameter *offset* is used to avoid u_l for $i \equiv 0 \bmod k$. In Step 9, the output of Step 7 is converted into a polynomial and added to Θ.

errors induced from the channel. To find the correct feedback polynomial in a noisy channel, Algorithm 2 is iteratively performed for L times in the same manner in [18]. However, even if Algorithm 2 is repeatedly performed, the incorrect feedback polynomial can still be obtained. For further improvement, in this paper, we propose verification of the feedback polynomial candidates using (10) to check whether the polynomial obtained from Algorithm 2 is a multiple of $c(x)$ or not.

In a noiseless channel, the inner product of an arbitrary vector and a vector in the vector space spanned by $(u_l)_{l=i}^{i-(q-1)}$, $i \not\equiv 0 \bmod k$ is 0 with a probability of 1/2. In addition, the inner product of $\boldsymbol{c}^{\gg j}$ and the vector in the vector space spanned by $(u_l)_{l=i}^{i-(q-1)}$, $i \not\equiv 0 \bmod k$ is always 0 because of (10). On the other hand, in a noisy channel, the inner product of $\boldsymbol{c}^{\gg j}$ and the vector in the vector space spanned by $(u_l)_{l=i}^{i-(q-1)}$, $i \not\equiv 0 \bmod k$ is 0 with a probability smaller than 1 because of the bit errors. However, it is still larger than 1/2. Using this probability gap, we can distinguish the right feedback polynomial candidates from the wrong ones and verify the feedback polynomial candidates to determine the correct feedback polynomial.

After verifying each feedback polynomial candidate, the GCD polynomial of all verified feedback polynomial candidates is determined as the correct feedback polynomial. We summarize the proposed blind estimation method of the feedback polynomial for the noisy channel in Algorithm 3. In Step 11, deg(θ) denotes the degree of the polynomial θ and the verification parameter R determines how many sequences are used for the verification of θ.

The number of iterations L and the verification parameter R affect the minimum length of the received sequence required to run Algorithm 3. If we denote the minimum length of the received sequence required to run Algorithm 3 as M, it can be obtained by

$$M = \max\{(n_{th} + L - 2)k + n_{th}, (R - 1)k + n_{th}\}. \quad (11)$$

In (11), the first term is the minimum length of the received sequence required to run Steps 4 to 9, and the second term is that for running Steps 12 to 14 in Algorithm 3. In practice, it is plausible to assume that $L > R$ because it is important to obtain as many feedback polynomial candidates as possible, and thus, we can rewrite (11) as

$$M = (n_{th} + L - 2)k + n_{th}. \quad (12)$$

Note that Algorithm 3 first finds as many feedback polynomial candidates as possible in Steps 4 to 9 using the basis of the orthogonal complement space and then determines the correct feedback polynomial in Steps 10 to 14 using the probability gap of the inner product.

The threshold TH, which is used to distinguish the right feedback polynomial candidates from the wrong ones in Step 14, affects the estimation performance of Algorithm 3. If TH is too small, the polynomial that is not a multiple of the correct feedback polynomial indeed can be included

TABLE 1. Feedback polynomials of the self-synchronous scrambler used in simulations for various polynomial degrees.

Degrees of polynomials (n)	Feedback polynomial ($c(x)$)
10	$x^{10}+x^3+1$
15	$x^{15}+x+1$
20	$x^{20}+x^6+x^4+x+1$
25	$x^{25}+x^{12}+x^4+x^3+1$
30	$x^{30}+x^{27}+x^{10}+x^9+1$

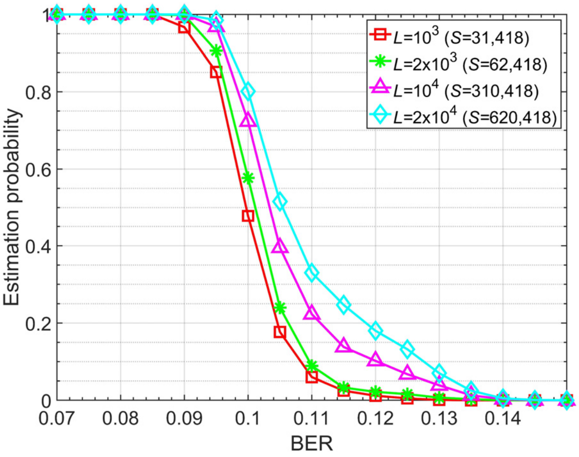

FIGURE 4. Estimation probability of Algorithm 3 versus BER for various L.

in Θ. On the other hand, if TH is too large, a multiple of the correct feedback polynomial cannot be included in Θ. Therefore, it is important to set TH to an appropriate value. After performing simulations by changing the values of TH, we find that Algorithm 3 shows satisfactory performance when TH is 0.55, and therefore, we set TH to 0.55 in the simulations.

IV. ESTIMATION PERFORMANCE

In this section, to validate the proposed method, we show the estimation probability of Algorithm 3 for various bit error rates (BER) in a binary symmetric channel. Furthermore, the computational complexity and the execution time of Algorithm 3 are investigated. Throughout the simulations, we set the verification parameter, R, to 3×10^3, the upper bound of the degree of the feedback polynomial, n_{th}, to $n + 5$, and the length of the spreading code, k, to 31, respectively. The feedback polynomials for various polynomial degrees, which are used in the simulations, are shown in Table 1.

We show the estimation probability of Algorithm 3 for various L to check the effect of L on the estimation performance in Fig. 4. In the simulations, we set n to 10 and L to 10^3, 2×10^3, 10^4, and 2×10^4, respectively. The length of the received sequence, S, is also described in parentheses with L in Fig. 4. From Fig. 4, we can observe that the estimation probability increases as L becomes large. In specific, the estimation probabilities of Algorithm 3 reach almost 0.9 at BERs of 0.093, 0.095, 0.097, and 0.099 for $L = 10^3$, 2×10^3, 10^4, and 2×10^4, respectively. This is because, as L increases, the probability of obtaining the multiples of the correct feedback polynomials increases in Steps 4 to 9 of Algorithm 3. From the simulation results, we can also confirm that there is a trade-off between the estimation probability and the amount of received data because as L becomes large, the receiver requires a larger amount of data to run Algorithm 3.

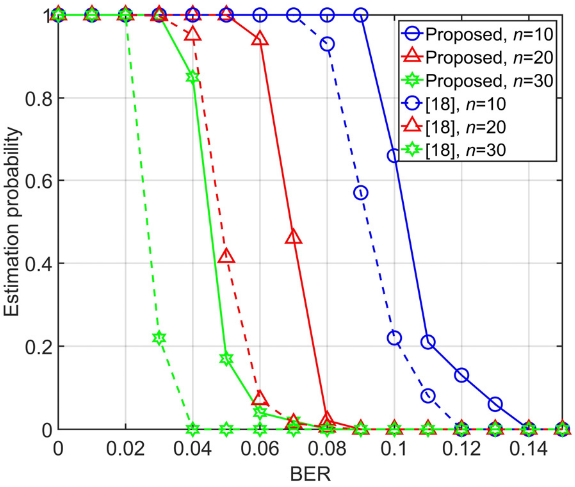

FIGURE 5. Estimation probability of Algorithm 3 (proposed) and Algorithm 2 in [18] for various BERs when $L = 10^4$.

To compare the performance, the estimation probabilities of Algorithm 2 in [18] are also given for the same parameters in Fig. 5. In the simulations, we set L to 10^4 for Algorithm 2 in [18] and Algorithm 3 of this paper, and the length of the received sequence, S, is set to 310,418 which is obtained from (12) when L is 10^4. From Fig. 5, we can see that the estimation probabilities of Algorithm 3 can reach around 0.9 at BERs of 0.09, 0.06, and 0.035 for the feedback polynomial degrees $n = 10$, 20, and 30, respectively, whereas estimation probabilities of Algorithm 2 in [18] reach almost 0.9 at BERs of 0.08, 0.041, and 0.021 for the feedback polynomial degrees $n = 10$, 20, and 30, respectively. From the results, we see that the proposed method outperforms the previous method in [18]. This is due to the fact that the proposed method can find more feedback polynomial candidates compared to [18] and has verifications, which result in better estimation probabilities.

Next, we show the computational complexity of Algorithm 3 in terms of the bitwise operations in Table 2, along with that of Algorithm 2 in [18]. From Table 2, we can see that the computational complexity of Algorithm 3 increases as the number of iterations L increases. Therefore, the execution time also increases as L becomes large. Compared to Algorithm 2 in [18], the complexity of Algorithm 3 slightly increases due to the verifications of the feedback polynomial

TABLE 2. Comparison of the computational complexities of Algorithm 3 and Algorithm 2 in [18].

Bitwise computational complexity			
Step	Algorithm 3	Step	Algorithm 2 in [18]
2	$O(S)$	1	$O\left(n_{th}^3 L+S\right)$
3-9	$O\left(n_{th}^3 L\right)$	2	-
10-14	$O\left(a n_{th}{}^2 R\right)$	3	$O\left(n_{th} \log^2 n_{th}\right)$
15	$O\left(n_{th} \log^2 n_{th}\right)$		
Total	$O\left(n_{th}^3 L+S+a n_{th}^2 R +n_{th} \log^2 n_{th}\right)$	Total	$O\left(n_{th}{}^3 L+S+n_{th} \log^2 n_{th}\right)$

a: Average number of polynomials in Step 5,
S: Bit length of the input sequence.

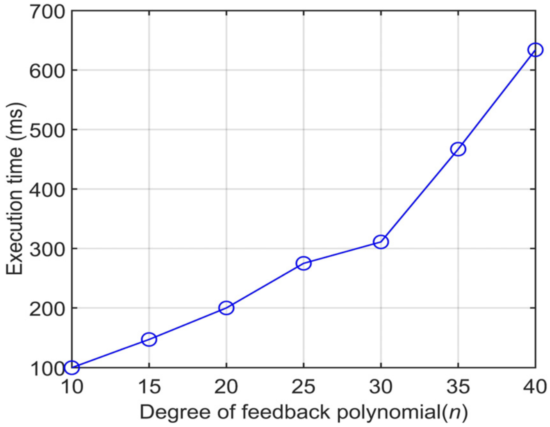

FIGURE 6. The execution time of Algorithm 3 for various feedback polynomial degrees (*n*).

candidates. However, in what follows, we will show that the execution time is still acceptable in a practical sense.

To check the execution time of Algorithm 3, we perform the simulations with an AMD Ryzen 5 3600 of 3.58 GHz and 32 GB RAM. We depict the results in Fig. 6, where the x-axis and y-axis represent the degree of the feedback polynomial n and time (ms), respectively. The execution time is measured by the average time of 100 runs when $L = 10^4$. As can be seen in Fig. 6, even when the degree of the feedback polynomial is 40, the execution time is shorter than 700ms, which is acceptable in practice.

V. CONCLUSION

In this paper, we proposed an improved algorithm for blind estimation of a self-synchronous scrambler using the orthogonal complement space without any bias condition of the received signals in DSSS systems. By applying the method for calculating the basis of the orthogonal complement space, we obtained as many feedback polynomial candidates of the scrambler as possible to improve the estimation performance. Considering the bit errors induced from a noisy channel, verifications for each feedback polynomial candidate were conducted, and then the correct feedback polynomial was estimated by calculating the GCD polynomial of all verified feedback polynomial candidates. Through computer simulations, we showed that the proposed method had superior performance compared to the conventional method in terms of the estimation probability. It is noteworthy that the execution time of the proposed method is practical, even if there is a slight increase in computational complexity compared to the previous method. Therefore, it is expected that the proposed method can be applied to a practical system.

In this paper, we assume that we can collect a sufficient amount of data to construct as many matrices as we need. Considering when the scant data are collected, future work could include efficient blind scrambler estimation for the cases where there is scant data.

ACKNOWLEDGMENT

(Yoonji Kim and Jungmin Kim contributed equally to this work.)

REFERENCES

[1] J. Lee, J. Kim, B. Kim, D. Yoon, and J. Choi, "Robust automatic modulation classification technique for fading channels via deep neural network," *Entropy*, vol. 19, no. 9, p. 454, Aug. 2017.

[2] L. Zhang, H. Liu, X. Yang, Y. Jiang, and Z. Wu, "Intelligent denoising-aided deep learning modulation recognition with cyclic spectrum features for higher accuracy," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 57, no. 6, pp. 3749–3757, Dec. 2021.

[3] B. Kwon, H. Song, and S. Lee, "Accurate blind Lempel-Ziv-77 parameter estimation via 1-D to 2-D data conversion over convolutional neural network," *IEEE Access*, vol. 8, pp. 43965–43979, 2020.

[4] J. Barbier, G. Sicot, and S. Houcke, "Algebraic approach for the reconstruction of linear and convolutional error correcting codes," *Int. J. Appl. Math. Comput. Sci.*, vol. 2, no. 3, pp. 113–118, Nov. 2006.

[5] R. Moosavi and E. G. Larsson, "Fast blind recognition of channel codes," *IEEE Trans. Commun.*, vol. 62, no. 5, pp. 1393–1405, May 2014.

[6] T. Xia and H.-C. Wu, "Novel blind identification of LDPC codes using average LLR of syndrome a posteriori probability," *IEEE Trans. Signal Process.*, vol. 62, no. 3, pp. 632–640, Feb. 2014.

[7] M. Jang, G. Kim, D. Kim, and D. Yoon, "Blind interleaver parameter estimation from scant data," *IEEE Access*, vol. 8, pp. 217282–217289, 2020.

[8] J. Oh, J. Jeong, Y. Jang, J. Lee, and D. Yoon, "Blind classification of line-coding schemes based on characteristic features," *IEEE Access*, vol. 5, pp. 9562–9567, 2017.

[9] D. Torrieri, *Principles of Spread-Spectrum Communication Systems*, Boston, MA, USA: Springer, 2005.

[10] M. Cluzeau, "Reconstruction of a linear scrambler," *IEEE Trans. Comput.*, vol. 56, no. 9, pp. 1283–1291, Sep. 2007.

[11] X.-B. Liu, S. N. Koh, X.-W. Wu, and C.-C. Chui, "Reconstructing a linear scrambler with improved detection capability and in the presence of noise," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 208–218, Feb. 2012.

[12] X.-B. Liu, S. N. Koh, C.-C. Chui, and X.-W. Wu, "A study on reconstruction of linear scrambler using dual words of channel encoder," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 3, pp. 542–552, Mar. 2013.

[13] Y. Ma, L. M. Zhang, and H. T. Wang, "Reconstructing synchronous scrambler with robust detection capability in the presence of noise," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 2, pp. 397–408, Feb. 2015.

[14] S. Han and M. Zhang, "A method for blind identification of a scrambler based on matrix analysis," *IEEE Commun. Lett.*, vol. 22, no. 11, pp. 2198–2201, Nov. 2018.

[15] X. Gu, Z. Zhao, and L. Shen, "Blind estimation of pseudo-random codes in periodic long code direct sequence spread spectrum signals," *IET Commun.*, vol. 10, no. 11, pp. 1273–1281, Jul. 2016.

[16] H. Xie, F. Wang, and Z. Huang, "Blind reconstruction of linear scrambler," *J. Syst. Eng. Electron.*, vol. 25, no. 4, pp. 560–565, 2014.

[17] D. Kim, J. Song, and D. Yoon, "On the estimation of synchronous scramblers in direct sequence spread spectrum systems," *IEEE Access*, vol. 8, pp. 166450–166459, 2020.
[18] D. Kim and D. Yoon, "Blind estimation of self-synchronous scrambler in DSSS systems," *IEEE Access*, vol. 9, pp. 76976–76982, 2021.
[19] G. Strang, *Introduction to Linear Algebra*, Wellesley, MA, USA: Wellesley-Cambridge Press, 1993.
[20] V. Shoup, *A Computational Introduction to Number Theory and Algebra*. Cambridge, U.K.: Cambridge Univ. Press, 2009.
[21] J. Von Zur Gathen and J. Gerhard, *Modern Computer Algebra*. Cambridge, U.K.: Cambridge Univ. Press, 2013.

YOONJI KIM (Member, IEEE) received the B.S. degree in electronic engineering from Hanyang University, Seoul, South Korea, in 2019, where she is currently pursuing the Ph.D. degree with the Department of Electronic Engineering. Her research interests include digital communication theory and wireless communications.

JUNGMIN KIM (Member, IEEE) received the B.S. degree in mathematics from Hanyang University, Seoul, South Korea, in 2020, where he is currently pursuing the Ph.D. degree in mathematics under the supervision of Prof. J. Song. His research interests include cryptanalysis of symmetric-key cryptography and zero knowledge proof systems.

JUNGHWAN SONG (Member, IEEE) received the B.S. degree from Hanyang University, Seoul, South Korea, in 1984, the M.S. degree from Syracuse University, NY, USA, in 1989, and the Ph.D. degree from the Rensselaer Polytechnic Institute, NY, USA, in 1993, all in mathematics. He was the Chairperson of Korea Cryptographic Forum. He is currently a Professor with the Department of Mathematics, Hanyang University. His current research interests include cryptanalysis of symmetric-key cryptography, mathematical optimization, and post quantum cryptography.

DONGWEON YOON (Senior Member, IEEE) received the B.S. *(summa cum laude)*, M.S., and Ph.D. degrees in electronic communications engineering from Hanyang University, Seoul, South Korea, in 1989, 1992, and 1995, respectively. From March 1995 to August 1997, he was an Assistant Professor with the Department of Electronic and Information Engineering, Dongseo University, Busan, South Korea. From September 1997 to February 2004, he was an Associate Professor with the Department of Information and Communications Engineering, Daejeon University, Daejeon, South Korea. Since March 2004, he has been on a Faculty Member of Hanyang University, where he is currently a Professor with the Department of Electronic Engineering and the Director of the Signal Intelligence Research Center. His research interests include digital communications theory and systems, detection and estimation, satellite and space communications, and communication forensics.