

# 잡음 환경에서 통계적 방법을 이용한 선형 피드백 시프트 레지스터 추정

김 동 영\*, 김 윤 지\*, 박 철 순\*\*, 송 정 환\*\*\*, 윤 동 원<sup>o</sup>

## Linear Feedback Shift Register Estimation Using Statistical Method in a Noisy Environment

Dongyeong Kim\*, Yoonji Kim\*, Cheol-sun Park\*\*, Junghwan Song\*\*\*, Dongweon Yoon<sup>o</sup>

### 요 약

비협력 통신환경에서는 채널부호, 인터리버, 확산부호, 선형 피드백 시프트 레지스터(Linear Feedback Shift Register, LFSR) 등을 추정해야 한다. 특히 LFSR에 의해 생성되는 의사 난수 수열을 추정하기 위해서는 일반적으로 BM(Berlekamp-Massey)알고리즘이 사용되는데, 잡음 환경에서는 이를 이용하더라도 오류로 인하여 LFSR을 추정하는 것이 어렵다. 본 논문에서는 잡음 환경에서 LFSR을 추정하기 위해 수집된 수열의 일부를 이용해 LFSR을 추정한 후 이를 이용하여 생성된 의사 난수 수열과 수집된 수열과의 오류 비트 개수의 차이를 비교함으로써 올바른 LFSR을 추정하기 위한 통계적 방법을 제안하고 추정 성능을 분석한다.

**Key Words** : Linear feedback shift register, m-sequence, Berlekamp-Massey algorithm, Synchronous scrambler, Feedback polynomial

### ABSTRACT

In non-cooperative scenario, channel code, interleaver, spreading code and linear feedback shift register(LFSR) should be estimated. In particular, the Berlekamp-Massey algorithm is generally used to estimate the pseudo-random number generated by the LFSR in error-free situation. However in a noisy environment, because of the errors, it is difficult to estimate the correct LFSR. In this paper, we propose the statistical method to estimate the LFSR in a noisy environment by comparing the number of errors due to the difference of the given sequence and generated sequence with the number of errors occurred by the noisy environment, and analyze the performance of estimation method.

※ 본 연구는 국방과학연구소 광대역저피탐 DSSS 신호 탐지 및 분석시험장치대 과제 수행 결과의 일부임

• First Author : Department of Mathematics, Research Institute for Natural Sciences, Hanyang University, wrskdy@hanyang.ac.kr, 정희원

◦ Corresponding Author : Hanyang University Department of Electronics and Computer Engineering, dwyoon@hanyang.ac.kr, 종신희원

\* Hanyang University Department of Electronics and Computer Engineering, natasha0826@hanyang.ac.kr, 정희원

\*\* Agency for Defense Development, helione@nate.com, 정희원

\*\*\* Department of Mathematics, Research Institute for Natural Sciences, Hanyang University, camp123@hanyang.ac.kr

논문번호 : 201912-327-0-SE, Received October 31, 2019; Revised January 8, 2020; Accepted January 11, 2020

## I. 서 론

대역확산(Spread Spectrum) 시스템에 사용되는 선형 피드백 시프트 레지스터(Linear Feedback Shift Register, LFSR)는 시프트 레지스터에 입력되는 값이 이전 상태 값들의 선형 함수로 표현되는 구조를 갖는다. 이러한 LFSR의 초기 값에 선형 함수, 즉 피드백 다항식을 적용하여 순차적으로 수열을 생성할 수 있다. 만약 이 때 적용된 피드백 다항식이 원시 다항식이라면 LFSR에 의해 생성된 수열은 m-sequence<sup>[1]</sup> (Maximum Length Sequence)라 한다. 이 외에도 LFSR로부터 생성되는 여러 수열들 간에 Decimation 또는 m-sequence간 XOR을 통해 KASAMI sequence<sup>[2]</sup>나 Gold sequence<sup>[3]</sup>를 생성할 수 있다. m-sequence는 고유의 수학적 특징을 기반으로 CDMA<sup>[4,5]</sup> (Code Division Multiple Access), 위성 항법<sup>[6]</sup>(GPS) 등 다양한 통신 시스템에서 사용되고 있다.

한편 비협력(Non-cooperative)통신 환경에서는 송신단에서 사용된 LFSR을 알 수 없기 때문에 수신된 수열만을 이용하여 LFSR을 블라인드 추정해야 한다.<sup>[7,8]</sup> LFSR로부터 생성된 수열에 잡음으로 인한 오류가 더해졌을 때, 원래의 수열을 생성하기 위한 LFSR을 추정하기 위하여 기존의 알고리즘<sup>[8]</sup>은 수신된 수열을 BM 알고리즘을 적용하기 위한 크기인 LFSR의 시프트 레지스터 길이의 2 배 크기의 비트열로 나눈 후에 각각의 비트열 단위별로 BM 알고리즘<sup>[9]</sup>을 적용하여 가장 많이 출력된 LFSR의 피드백 다항식을 올바른 피드백 다항식으로 추정하였다. 그러나 이 방법은 LFSR의 단 수가 크거나 잡음 환경에서 오류 확률이 큰 경우 올바른 추정을 위해 필요한 수신 비트 수가 기하급수적으로 증가하게 된다.

본 논문에서는 수신된 수열의 일부분을 BM 알고리즘의 입력 값으로 하여 LFSR의 피드백 다항식을 구하고, 이를 이용하여 생성한 수열과 처음에 주어진 수열 전체의 차이를 이용하여 올바른 피드백 다항식을 추정하는 새로운 방법을 제시한다. 또한 제안한 알고리즘을 수학적으로 분석하고 모의실험을 통해 두 알고리즘의 추정 성능을 비교한다.

## II. LFSR의 피드백 다항식 추정 방법

잡음 환경에서 올바른 LFSR의 피드백 다항식을 추정하기 위해 기존 방법은  $S_{len}$  비트 길이의 수신 수열  $S$ 를 각각 LFSR의 단 수  $L$ 의 2 배의 길이인  $2L$  길

이로 나뉘어 BM 알고리즘을 적용하고, 출력된 다항식들 중 가장 많이 출력된 피드백 다항식을 올바른 피드백 다항식으로 추정하였다<sup>[8]</sup>. 이 방법으로 피드백 다항식 추정이 가능하기 위해서는 BM 알고리즘에 의해 올바른 피드백 다항식이 출력되는 횟수가 잘못된 피드백 다항식이 출력되는 횟수보다 많아야 한다. 이 방법은 채널 상에 오류비트가 증가하거나 LFSR의 시프트 레지스터 단 수가 증가함에 따라 추정에 필요한 비트 수가 급증하게 된다.

이 장에서는 미리  $L$ 이 특정되었다고 가정할 때, 추정에 필요한 비트 수를 줄이고, 추정 성능을 높이기 위하여 오류 비트의 수의 차이를 이용하여 올바른 피드백 다항식과 잘못된 피드백 다항식을 구분하도록 하는 방법과 수신 수열에서 길이가  $2L$ 인 연속된 모든 비트열들에 대하여 BM 알고리즘을 적용하는 개선된 기법을 제안하고 성능을 분석한다.

### 2.1 오류비트의 차이를 이용한 LFSR 추정 알고리즘

우선 BM 알고리즘으로 얻은 다항식을 올바른 피드백 다항식으로 가정하고, BM 알고리즘에 입력한 난수열을 초기 값으로 하여  $ML$ (여기서  $M$ 은 자연수) 비트 길이의 난수열을 생성한다. 만약, 출력된 다항식이 올바른 피드백 다항식이라면,  $ML$  비트 길이의 난수열은 잡음에 의해 오류가 더해진 비트를 제외하고 원래의 수열  $S$ 와 동일할 것이다. 즉, BER(Bit Error Rate)  $\beta$ 에 따라 두 난수열 간에는 평균적으로  $\beta ML$ 만큼의 서로 다른 비트들이 존재할 것이다. 반면, 출력된 다항식이 잘못된 피드백 다항식이라면,  $ML$  비트 길이의 난수열과 처음에 주어진 난수열  $S$ 는 서로 독립이므로, 각 비트가 같을 확률은  $1/2$ 이며, 따라서 두 난수열 간에는 평균적으로  $ML/2$ 만큼의 서로 다른 비트들이 존재할 것이다. 생성된  $ML$  비트 길이 난수열과 원래 주어진 난수열  $S$ 간에서 서로 다른 비트들의 수  $H$ 에 대하여, BM 알고리즘에서 올바른 피드백 다항식을 출력한 경우의  $H$ 인  $H|_C$ 와 그렇지 않은 경우의  $H$ 인  $H|_{\bar{C}}$ 는 다음과 같은 정규 분포를 따르게 된다. 여기서  $C$ 는 BM 알고리즘에서 올바른 피드백 다항식을 출력한 경우를,  $\bar{C}$ 는 그렇지 않은 경우를 나타낸다.

$$H|_C \sim \mathcal{N}(\beta ML, \beta(1-\beta)ML) \quad (1)$$

$$H|_{\bar{C}} \sim \mathcal{N}\left(\frac{1}{2}ML, \frac{1}{4}ML\right) \quad (2)$$

식 (1)과 (2)에서  $H|_C$ 와  $H|_{\bar{C}}$ 의 평균은  $(\frac{1}{2}-\beta)ML$ 만큼 차이가 난다. 예를 들어  $\beta=0.2$ 인 경우, 두 평균의 차는  $0.3ML$ 이므로 매우 큰 차이를 보인다. 따라서 이를 이용하여 **BM** 알고리즘에서 출력된 다항식이 올바른 피드백 다항식인지, 잘못된 피드백 다항식인지 명확하게 구분할 수 있다. 제안하는 알고리즘은 다음과 같은 과정으로 구성된다.

$H|_C$ 와  $H|_{\bar{C}}$ 의 확률 질량 함수를  $f_1$ 과  $f_2$ 라 할 때, 이들은 연속적이지 않으나 연속적인 형태로 근사할 수 있으며 일반적으로 정규분포의 확률 밀도 함수는 기댓값과 표준편차를 이용하여 계산이 가능하다.  $H|_C < H|_{\bar{C}}$ 일 확률  $\Pr[H|_C < H|_{\bar{C}}]$ 는 다음과 같다.

$$\Pr[H|_C < H|_{\bar{C}}] = \sum_{i=0}^{\infty} \left[ f_1(i) \sum_{j=i+1}^{\infty} f_2(j) \right] \quad (3)$$

실제로 정규 분포에 대한 확률 질량 함수  $f_1$ 과  $f_2$ 를 식 (3)에 대입하여  $\Pr[H|_C < H|_{\bar{C}}]$ 를 계산할 수 있으나, 매우 복잡하므로 이 논문에서는 계산하지 않는다. 그러나 이 확률이 매우 높다는 것은  $H|_C$ 와  $H|_{\bar{C}}$ 의 신뢰 구간을 통해 확인할 수 있다. 식 (1)과 (2)로부터  $H|_C$ 와  $H|_{\bar{C}}$ 의 유의수준 0.01에 대한 신뢰 구간은 다음과 같다.

$$\left[ \beta ML - Z_{0.01/2} \sqrt{\beta(1-\beta)ML}, \beta ML + Z_{0.01/2} \sqrt{\beta(1-\beta)ML} \right] \quad (4)$$

$$\left[ \frac{1}{2}ML - Z_{0.01/2} \frac{\sqrt{ML}}{2}, \frac{1}{2}ML + Z_{0.01/2} \frac{\sqrt{ML}}{2} \right] \quad (5)$$

예를 들어  $ML=100$ 이라면 식 (4), (5)의 신뢰계수  $Z_{0.005}=2.58$ 로부터 두 구간은 각각  $[100\beta - 25.8\sqrt{\beta(1-\beta)}, 100\beta + 25.8\sqrt{\beta(1-\beta)}]$ 와  $[50 - 12.9, 50 + 12.9]$ 가 된다. 만약  $\beta=0.25$ 라면 식 (4)의 상한은 36.2가 되고, 식 (5)의 하한은 37.1이 되므로, 이러한 경우 99% 이상의 확률로  $H|_C$ 가  $H|_{\bar{C}}$ 보다 작게 된다. 식 (4)의 상한과 식 (5)의 하한의 차이는  $ML$ 이 증가하거나  $\beta$ 가 감소하게 되면 더 커지게 된다. 따라서  $ML \geq 100$ 이고  $\beta \leq 0.25$ 인 상황에서는 99% 이상의 확률로  $H|_C < H|_{\bar{C}}$ 가 성립한다.

본 절에서 제안하는 추정 알고리즘은 다음과 같이 구성된다.

오류비트의 차이를 이용한 LFSR 추정방법	
1.	$S_{len}$ 길이의 난수열 $S$ 를 길이가 $2L$ 인 난수열로 나눈다.
2.	각각의 $2L$ 길이 난수열에 대하여 다음을 수행한다. <ul style="list-style-type: none"> <li>2-1. <b>BM</b> 알고리즘에 <math>2L</math> 비트 길이 난수열을 입력하여 다항식을 구한다.</li> <li>2-2. 구한 다항식을 피드백 다항식으로, <math>2L</math> 비트 길이 난수열을 초기값으로 하여, <math>ML</math> 비트 길이 난수열을 생성한다.</li> <li>2-3. <math>ML</math> 비트 길이 난수열과 이에 대응하는 위치의 주어진 난수열 <math>S</math>를 <b>XOR</b>하고, <b>XOR</b>된 비트열의 해밍 무게를 측정한다.</li> </ul>
3.	가장 낮은 해밍 무게를 갖는 피드백 다항식을 올바른 피드백 다항식으로 출력한다.

한편 올바른 피드백 다항식이 **BM** 알고리즘에 의해 출력되는 경우가 1 번이라도 발생한다면, 올바른 피드백 다항식은 잘못된 피드백 다항식과 구분될 수 있으므로 올바른 피드백 다항식을 추정할 수 있다. 그러나 만약  $\bar{C}$  인 경우만 발생한다면, 즉, 올바른 피드백 다항식이 **BM** 알고리즘에 의해 단 한 차례도 출력되지 않는다면 잘못된 **LFSR**의 피드백 다항식을 추정하게 될 것이다. 따라서 제안하는 알고리즘을 통해 올바른 피드백 다항식을 추정할 확률은 **BM** 알고리즘이 올바른 피드백 다항식을 한 번 이상 출력할 확률과 같으며, 이 확률을 높이면 추정 성능이 향상된다.

### 2.2 LFSR 추정 성능 개선 기법 제안

앞 절에서 제안한 오류비트의 수를 이용한 **LFSR** 추정 알고리즘의 성능을 보다 향상시키기 위해 수열  $S$ 에서 길이가  $2L$ 인 연속된 모든 비트열들에 대하여 **BM** 알고리즘을 적용하는 개선된 기법을 제시한다. 이 경우 가장 오른쪽의  $2L-1$  비트를 제외하고 모든 비트 위치에서 연속된  $2L$  비트열을 생성할 수 있으므로, 총  $S_{len} - 2L + 1$ 번 **BM** 알고리즘에 적용할 수 있다. 이 때, 단 하나라도 오류가 없는  $2L$  비트 길이 비트열이 나올 확률은, 0과 1로 이루어진 비트열에서 각 비트마다 1이 등장할 확률이  $\beta$ 라고 할 때, 0으로 이루어진 가장 긴 제로 런(**Zero Run**)의 길이가  $2L$  이상일 확률과 같다. 이 확률을 구하는 것은 어렵지만, 가

장 높은 확률로 등장하는 최대 길이 제로 런의 길이를 예측하는 것은 가능하다. 비트열의 길이가  $n$ 이고, 0이 등장할 확률이  $p$ 일 때, 가장 긴 제로 런의 길이  $R_n$ 은 다음으로 근사된다.<sup>[10]</sup>

$$R_n = \log_{1/p}(n(1-p)) \quad (6)$$

또한 식 (6)에서의 값보다 더 긴 길이의 제로 런이 등장할 확률은 더 짧은 길이의 제로 런이 등장할 확률보다 더 크다.<sup>[10]</sup> 따라서 만약  $2L$ 이  $R_n$ 보다 작거나 같은 경우, 우리는 50% 이상의 확률로 BM 알고리즘에 오류가 없는 비트열이 최소 1개 이상 입력되어 올바른 피드백 다항식이 최소 1 번 이상 등장하게 될 것으로 기대할 수 있다. 실험을 통해 평균적으로 가장 긴 길이의 제로 런은 식 (6)의 값보다 1 정도 더 큰 값을 갖는 것을 확인하였다. 제시한 기법을 사용하면, 예를 들어  $S_{len} = 8192$ ,  $L = 16$ ,  $\beta = 0.2$ 일 때, 식 (6)으로부터 가장 긴 제로 런의 길이  $R_{S_{len}} = -\log_{1-0.2}(S_{len} \cdot 0.2) = 33.17$ 이며 이는  $2L = 32$ 보다 길다. 따라서 이 경우 높은 확률로 BM 알고리즘에서 한 번 이상 올바른 피드백 다항식을 출력하게 된다. 따라서 제시한 기법을 적용한다면 훨씬 더 좋은 추정 성능을 기대할 수 있다.

### III. 모의 실험 및 성능 분석

이 장에서는 채널의 BER에 따른 각 알고리즘들의 LFSR 피드백 다항식 추정 성능을 비교한다. 또한  $L$ ,  $\beta$ ,  $S_{len}$ , 그리고 오류 개수 차이를 고려해야 하는 비트열의 길이를 결정하는 매개변수인  $M$ 에 따른 추정 성능의 차이를 분석한다. 실험은 1000번의 시도를 통해 추정 성공률을 계산하였다. 그리고 편의를 위해 기존의 추정 방법을 Conventional, 오류비트의 차이를 이용한 추정 방법을 Proposed#1, 성능 향상 기법을 Proposed#1에 적용한 추정방법을 Proposed#2 라고 나타내기로 한다.

$L = 6, 8, 10, 12, 14, 16$ 일 때, 각 알고리즘 별로 추정 확률을 그림 1에 도시하였다. 여기서  $S_{len} = 128L$ 이며,  $M = 10$ 이다.  $\beta = 0.05$ 인 경우, 알고리즘에 상관없이 추정 확률이 1이며 그 외의 경우에서  $L$ 이나  $\beta$ 가 증가함에 따라 추정 확률이 감소함을 알 수 있다.

$S_{len}$ 이 증가함에 따라 제안한 방법들(Proposed#1, Proposed#2)의 추정 성능이 좋아지는지 확인하기 위

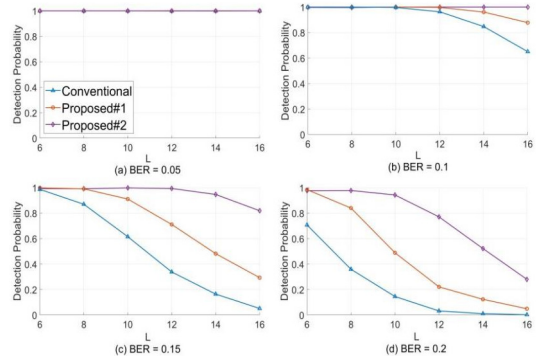


그림 1. BER에 따른 각 알고리즘 별 추정 확률 ( $S_{len} = 128L$ ,  $M = 10$ )  
 Fig. 1. Detection performances of each algorithm with different BER ( $S_{len} = 128L$ ,  $M = 10$ )

하여  $S_{len}$ 에 따른 각 알고리즘 별 추정 성능을 실험적으로 확인하여 그림 2에 나타내었다. 여기서  $M = 10$ ,  $\beta = 0.2$ ,  $L = 16$ 이다. 그림 2에서  $S_{len}$ 이 증가함에 따라 오류비트의 차이를 이용하는 추정 방법 Proposed#1과 여기에 개선된 기법을 적용한 Proposed#2 모두 추정 확률이 크게 증가하는 것을 확인할 수 있는데, 이는  $S_{len}$ 이 증가함에 따라 BM 알고리즘에서 올바른 피드백 다항식을 하나 이상 찾을 확률이 크게 증가하기 때문이다.

그림 3은 오류 비트 수의 차이를 증가시키기 위해  $M$ 을 증가시켰을 때, 추정 확률에 영향을 주는지 확인하기 위해  $M = 50$ 일 때의 추정 성능을 나타낸 것이다. 여기서  $S_{len} = 128L$ ,  $\beta = 0.2$ 이다. 그림 3에서 확인할 수 있듯이, 제안 방법들의 성능은 그림 1(d)의 성능과 큰 차이가 없다. 이는 식 (4)와 (5)에서 알 수 있듯이 BM 알고리즘에서 올바른 피드백 다항식을 하나

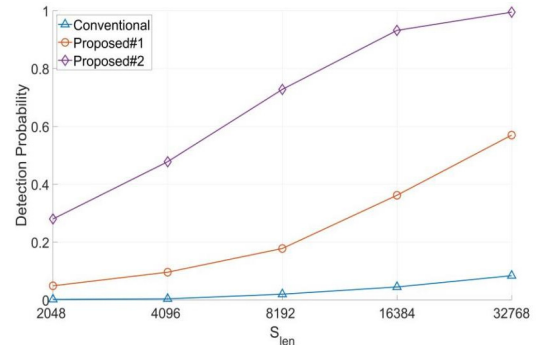


그림 2. 수열 S의 길이에 따른 추정 확률( $M = 10$ ,  $\beta = 0.2$ ,  $L = 16$ )  
 Fig. 2. Detection performances for each algorithm with the various length of S ( $M = 10$ ,  $\beta = 0.2$ ,  $L = 16$ )

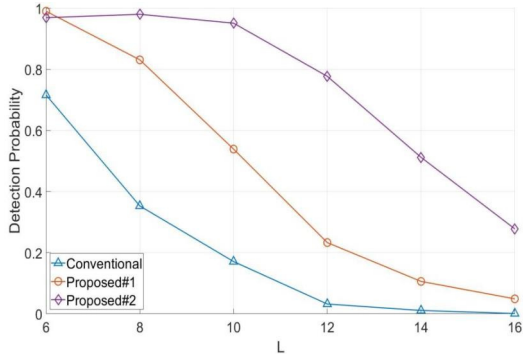


그림 3. M=50인 경우에 추정 확률( $S_{len} = 128L, \beta = 0.2$ )  
 Fig. 3. Performance for M = 50( $S_{len} = 128L, \beta = 0.2$ )

라도 출력한다고 가정했을 때,  $ML \geq 100$ 이면 올바른 추정이 가능하기 때문이다.

#### IV. 결 론

본 논문에서는 잡음 환경에서 LFSR의 파라미터를 추정하기 위한 통계적인 방법을 제시하고 실험을 통해 성능을 증명하였다. 기존의 방법은 수신된 수열의 길이가  $2L$ 인 수열로 나누어 BM 알고리즘을 적용한 뒤, 가장 많이 출력된 피드백 다항식을 올바른 다항식으로 추정하는 방법을 사용하였다. 하지만 이러한 방식은 BER과 LFSR의 단 수  $L$ 이 증가함에 따라 추정 확률이 크게 낮아지는 문제가 있었다.

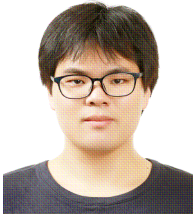
이를 해결하기 위하여 본 논문에서는 BM 알고리즘으로부터 피드백 다항식을 구한 후, 이 피드백 다항식으로부터 생성된 수열을 수신된 수열과 비교하여 오류가 가장 적은 수열을 생성하는 피드백 다항식을 올바른 다항식으로 추정하는 알고리즘을 제안하고  $ML \geq 100$ 이고  $\beta \leq 0.25$ 일 때, 99% 이상의 확률로 올바른 피드백 다항식과 잘못된 피드백 다항식을 구분할 수 있음을 수학적으로 보였다. 그리고 길이가  $2L$ 인 연속된 모든 비트열들 BM 알고리즘에 적용하는 개선된 기법을 적용하여 성능을 개선하였다.

모의 실험을 통해 본 논문에서 제안한 방법이 0.1 이상의 높은 BER과 16 이상의 높은 시프트 레지스터 단 수  $L$ 에서 기존의 방법보다 월등한 추정 성능을 보이며, 수열  $S$ 의 길이가 길어질수록 제안한 방법과 기존 방법의 추정 성능 차이가 커지는 것을 확인하였다.

#### References

- [1] S. W. Golomb and G. Gong, *Signal design for good correlation: for wireless communication, cryptography, and radar*, Cambridge University Press, 2005.
- [2] T. Kasami, "Weight distribution formula for some class of cyclic codes," Coordinated Science Laboratory Report, no. R-285, Apr. 1966.
- [3] R. Gold, "Optimal binary sequences for spread spectrum multiplexing," *IEEE Trans. Inf. Theory*, vol. IT-13, pp. 61-621, Oct. 1967.
- [4] J. G. Proakis and M. Salehi, *Digital Communications*, vol. 4, pp. 593-620, New York: McGraw-hill, 2001.
- [5] K. Feher, *Wireless digital communications: Modulation & spread spectrum applications*, Prentice-Hall Inc., 1995.
- [6] B. W. Parkinson, P. Enge, P. Axelrad, and J. J. Spilker Jr., "Global positioning system: Theory and applications," *Am. Inst. Aeronautics and Astronautics*, vol. 2, 1996.
- [7] C. Park, S. Lim, J. Lee, and J. Choi, "Performance of multi-antenna combining based uplink WCDMA scrambling code identification scheme in fading channels," in *Proc. KICS*, pp. 478-479, Jan. 2017.
- [8] M. Jang, S. Ahn, U. Jung, and D. Yoon, "Estimation of linear feedback shift register in noisy environments," in *Proc. KIEES Winter Conf.*, p. 39, Feb. 2019.
- [9] J. L. Massey, "Shift-register synthesis and BCH decoding," *IEEE Trans. Inf. Theory*, vol. IT-15, no. 1, pp. 122-127, Jan. 1969.
- [10] M. F. Schilling, "The longest run of heads," *The College Math. J.*, vol. 21, no. 3, pp. 196-207, 1990.

**김 동 영 (Dongyeong Kim)**



2013년 2월 : 한양대학교 수학과 학사 졸업  
2020년 2월 : 한양대학교 수학과 박사 졸업  
2020년 3월 현재 : 한양대학교 수학과 강사

<관심분야> 블록암호 분석, 양자 암호, 통신 공학  
[ORCID:0000-0001-5369-2424]

**송 정 환 (Junghwan Song)**



1984년 2월 : 한양대학교 수학과 졸업  
1989년 5월 : Syracuse 대학교 석사  
1993년 5월 : Rensselaer Polytechnic Institute  
2020년 3월 현재 : 한양대학교 수학과 교수

<관심분야> 최적화 기법, 블록암호 분석, 양자 암호  
[ORCID:0000-0002-8802-8141]

**김 윤 지 (Yoonji Kim)**



2019년 2월 : 한양대학교 융합전자공학부 학사 졸업  
2019년 2월~현재 : 한양대학교 전자컴퓨터통신공학과 석박사과정  
<관심분야> 블라인드 복조, 통신 공학

[ORCID:0000-0003-4247-5795]

**윤 동 원 (Dongweon Yoon)**



1989년 2월 : 한양대학교 전자통신공학과 (공학사)  
1992년 2월 : 한양대학교 전자통신공학과 (공학석사)  
1995년 8월 : 한양대학교 전자통신전파공학과 (공학박사)  
2020년 3월 현재 : 한양대학교 융합전자공학부 교수

<관심분야> 무선통신, 위성 및 우주통신  
[ORCID:0000-0001-9631-3500]

**박 철 순 (Cheol-sun Park)**



1989년 2월 : 경기대학교 전자계산학과 학사  
1991년 2월 : 인하대학교 전자계산공학과 석사  
1997년 5월 : 전자계산조직응용기술사  
2007년 2월 : 충남대학교 정보통신공학과 박사

1991년 2월~현재 : 국방과학 연구소 책임연구원  
<관심분야> 신호처리, 통신응용  
[ORCID:0000-0002-3678-4041]