
페이지 쉬프터 기반의 의사 난수 패턴 생성기

조성진* · 최언숙** · 황윤희*

Pseudo Random Pattern Generator based on phase shifters

Sung-Jin Cho* · Un-Sook Choi** · Yoon-Hee Hwang*

이 논문은 2009학년도 부경대학교의 지원을 받아 수행된 연구임(PK-2009-26)

요 약

패턴생성기로 LFSR(linear feedback shift register)은 기계 자체에 고유의 선형의존성이 있어 패턴을 생성함에 있어 비트의 위치를 이동시켜 수열을 생성하기 때문에 생성되는 패턴들의 상관관계가 높고 따라서 오류 검출률이 낮아지게 된다. 이런 문제점을 해소하기 위하여 scan chain 사이에 XOR 게이트의 조합으로 구성된 페이지 쉬프터를 장착하여 출력 테스트 패턴의 난수성을 높임으로써 LFSR 고유의 선형의존성을 줄이고 오류검출률을 높이는 연구가 활발히 진행되어 왔다. 본 논문에서는 PRPG(pseudo random pattern generator)로서 특성다항식을 원시다항식으로 갖는 LFSR을 사용하여 어떤 임의의 두 채널에서 출력되는 이진 수열의 선형의존성을 줄이기 위한 방법으로 적절한 탭 수를 유지하며 최소의 위상이동차를 보장하는 페이지 쉬프터를 갖는 LFSR 기반의 PRPG를 구성하는 방법을 제안한다. 제안된 알고리즘에 따라 페이지 쉬프터를 구성하면 기존의 방법보다 페이지 쉬프터를 훨씬 빨리 구성할 수 있는 장점이 있다.

ABSTRACT

Since an LFSR(linear feedback shift register) as a pattern generator has solely linear dependency in itself, it generates sequences by moving the bit positions for pattern generation. So the correlation between the generated patterns is high and thus reduces the possibility of fault detection. To overcome these problems many researchers studied to have goodness of randomness between the output test patterns. In this paper, we propose the new and effective method to construct phase shifter as PRPG(pseudo random pattern generator).

키워드

페이지 쉬프터, 위상이동차, LFSR, BIST, PRPG

Key word

Phase shifter, Phase shift, LFSR, BIST, PRPG

* 부경대학교
** 동명대학교 (교신저자)

접수일자 : 2009. 11. 05
심사완료일자 : 2009. 11. 30

I. 서 론

컴퓨터, 무선통신, 네트워크 장비, 휴대용 전자 기기 등의 급속한 확산 및 발전과 함께 반도체 산업은 크게 성장하였다. 최근 아날로그 회로, DSP(digital signal processor), 프로세서 및 메모리가 하나의 칩에 집적된 다양한 SoC(system on chip) 제품이 출시되고 있으며, 앞으로도 더욱 저렴한 가격으로 더 많은 기능을 갖는 SoC 제품에 대한 요구가 더욱 증대될 것이다. 이러한 반도체 제품을 테스트 하는 기술은 아직까지 고가의 외부 테스트 장비에 의존하고 있으나 회로의 복잡도 및 성능이 증가함에 따라 외부 테스트 장비가 갖는 한계는 더욱 확연해지고 있다. BIST(built-in self test)는 디지털 시스템을 시험하는데 있어 그동안 사용되던 외부장착 시험기에 대한 대안이다. BIST는 테스트 대상이 되는 칩 자체에 테스트 패턴을 생성하고 그 응답을 분석하는 기능을 내장시켜 테스트를 수행하는 방법이다. 이는 자체시험회로를 내장하므로 소요면적이 커지는 단점이 있지만 시험에 따른 복잡도가 크게 줄고 모듈별로 가장 적합한 시험이 가능하다. 또한 비용 면에 있어서도 비싼 외부 시험장치를 쓰지 않고서도 빠른 시간 내에 시험을 완료할 수 있다는 장점을 가지고 있다. 패턴생성기로 가장 널리 이용되고 있는 LFSR은 기계 자체에 고유의 선형의존성이 있어 패턴을 생성함에 있어 난수성이 떨어진다[1-2]. LFSR은 비트의 위치를 한 칸씩 이동시켜 수열을 생성하기 때문에 생성되는 패턴들의 상관관계가 높고 따라서 오류검출률이 낮아지게 된다. 이런 문제점을 해소하기 위하여 scan chain 사이에 XOR 게이트의 조합으로 구성된 페이지 쉬프트를 장착하여 출력 테스트 패턴의 난수성을 높임으로써 LFSR 고유의 선형의존성을 줄이고 오류검출률을 높이는 연구가 활발히 진행되어 왔다[3-10]. Rajski와 Tyszer는 조직적인 페이지 쉬프트를 자동으로 합성하는 방법을 처음으로 제안하였다[3]. 페이지 쉬프트는 패턴생성기와 scan chain 사이에 장착된 XOR 게이트들의 네트워크이다. 페이지 쉬프트의 주된 기능은 다음과 같다.

- 각 채널에서 출력되는 이진 수열간의 원하는 최소 위상 이동차 값을 보장하는 것
- 패턴생성기의 구조적인 의존성을 제거하는 것
- 어떤 임의의 두 채널에서 출력되는 이진 수열의 선형의존성을 줄이는 것

Kagaris는 페이지 쉬프트에서 사용되는 탭 수의 상한선과 패턴생성기로 만들어진 단계들 사이의 위상이동차의 하한선을 정하고 LHCA(linear hybrid cellular automata)나 LFSR과 관계없이 사용될 수 있는 페이지 쉬프트를 제시했다[9]. 그러나 Kagaris가 제안한 방법은 원하는 페이지 쉬프트 H 를 구성하기 위하여 이러한 적절한 벡터를 선택하는 과정에서 부적합 벡터를 너무 많이 전이시키며 확인하는 과정을 거치게 된다.

본 논문에서는 PRPG로서 LFSR의 난수성을 높이기 위하여 LFSR에 장착할 적용될 수 있는 새롭고 효과적인 페이지 쉬프트를 구성하는 방법을 제안한다. 이 방법은 기존의 방법에 비해 구현하는 것이 상당히 효율적이고 빠르다.

II. 배경지식 및 기존연구

BIST기법을 이용하여 회로를 검사하기 위해서는 검사입력을 자체 생성해야 한다. LFSR은 폴리플롭과 XOR 게이트로 구성되는데 특성다항식을 원시다항식으로 갖는 LFSR을 사용하면 모든 검사입력이 같은 확률로 생성되며 반복되지 않도록 하는 의사 난수 테스트 패턴(pseudo random test pattern)을 생성할 수 있다[11]. 이러한 LFSR은 XOR의 위치에 따라 2가지로 나타나는데 그림 1과 같다. 여기서 c_i 는 이진 상수로 $c_i = 0$ 은 끊어짐 상태를 1은 연결된 상태를 나타낸다. LFSR은 입력순서에 따라 출력순서와 출력부호를 결정하는 특성다항식을 갖는데 그림 1(a)에서 특성다항식은 $c(x) = 1 + c_1x + c_2x^2 + \dots + c_nx^n$ 으로 정의된다.

n 개의 폴리플롭으로 구성된 n 차 LFSR의 상태전이는 동반행렬과 초기 상태벡터를 이용하여 표현할 수 있다. n 차 원시다항식(primitive polynomial)

$$c(x) = 1 + c_1x + c_2x^2 + \dots + c_{n-1}x^{n-1} + x^n$$

를 특성다항식으로 갖는 외부 XOR LFSR의 동반행렬 $M_{e,x}$ 와 내부 XOR LFSR의 동반행렬 $M_{i,n}$ 는 다음과 같다. X_i 가 시간 i 에서의 LFSR의 상태벡터라 하면 다음 상태 X_{i+1} 은 $X_{i+1} = M_{e,x}X_i$ 또는 $X_{i+1} = M_{i,n}X_i$ 이다.

$$M_{ex} = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & 1 \\ c_0 & c_1 & c_2 & \dots & c_{n-2} & c_{n-1} \end{bmatrix}, M_{in} = \begin{bmatrix} c_{n-1} & 1 & 0 & \dots & 0 & 0 \\ c_{n-2} & 0 & 1 & \dots & 0 & 0 \\ c_{n-3} & 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ c_1 & 0 & 0 & \dots & 0 & 1 \\ c_0 & 0 & 0 & \dots & 0 & 0 \end{bmatrix}$$

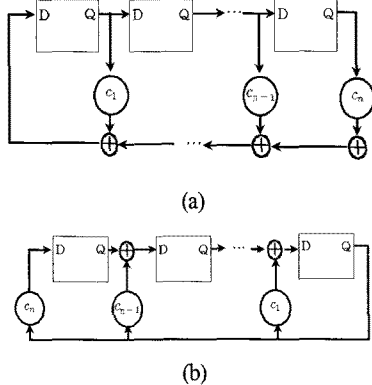


그림 1. LFSR구조
 (a) 외부 XOR를 이용한 LFSR
 (b) 내부 XOR를 이용한 LFSR
 Fig. 1. Structure of LFSR
 (a) LFSR using external XOR
 (b) LFSR using internal XOR

예를 들어 특성다항식이 $c(x) = x^4 + x + 1$ 인 내부 XOR LFSR의 동반행렬은 다음과 같다.

$$M_{in} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

$M(=M_{in})$ 에 의한 $(0,0,1,1)^t$ 의 다음 상태는 $M(0,0,1,1)^t = (0,1,1,0)^t$ 이다. 여기서 이렇게 얻어진 상태들을 행벡터로 나열하면 표1과 같다. 여기서 각 열은 같은 4차 원시다항식에 의해 생성되는 최대주기의 의사 난수열이다. 임의의 두 열에서 출력된 수열을 비교하면 한 출력수열은 다른 출력수열의 위치를 이동함으로써 얻을 수 있다. 이것을 위상이동차(phase shift)라고 한다.

<정의 1> 시간 t 에서 i 번째 열의 출력수열을 s_i^t 라 할 때, i 열에 대한 j 열의 위상이동차 h 는 다음과 같이 정의

한다.

$$s_j^{t+h} = s_i^t$$

표 1의 열들 사이의 위상이동차는 첫째 열에 대한 둘째 열의 위상이동차와 둘째 열에 대한 셋째 열의 위상이동차는 1이고, 셋째 열에 대한 넷째 열의 위상이동차는 12이다.

표 1. 4비트 LFSR의 상태전이
 Table 1. State Transition of 4 bit LFSR

	0123
0	0011
1	0110
2	1100
3	1011
4	0101
5	1010
6	0111
7	1110
8	1001
9	1101
10	1000
11	0001
12	0010
13	0100
14	1000

이와 같이 LFSR은 구조적으로 각 셀에서 출력되는 출력수열 사이에 강한 상관관계를 가진다. 이러한 문제를 해결하기 위해 Kagaris는 페이지 쉬프터에서 사용되는 탭 수의 상한선과 패턴생성기로 만들어진 단계들 사이의 위상이동차의 하한선을 정하고 LHCA나 LFSR과 관계없이 사용될 수 있는 페이지 쉬프터를 제안했다[4]. 주어진 LFSR에서 출력되는 수열 사이에 최소한의 위상이동차(L)를 보장하면서 적절한 수준의 탭 수(B)로 이루어진 페이지 쉬프터를 설계하기 위해 Kagaris는 LFSR에 상태벡터(X_t)를 가지고 상태를 L 단계 만큼 전이시킨다. 이 때 얻은 상태벡터(X_L)의 1의 수가 B 이하이면 X_L 은 페이지쉬프터(H)의 한 행이 된다. 그런데 X_L 의 1의 수가 B 를 초과하면 상태를 한 단계씩 전이시키면서 1의 수가 B 이하가 되는 상태벡터를 H 의 한 행으로 선택한다. 그러나 Kagaris가 제안한 방법은 원하는 페이지 쉬프터 H 를 구성하기 위하여 이러한 적절한 벡터를 선택하는 과정에서 부적합 벡터를 너무 많이 전이시키며 확인하는 과정을 거치게 된다. 따라서 이러한 문제점을 효과적으로 해결하는 방법을 다음 절에서 소개한다.

III. 페이지 쉬프트의 설계

LFSR은 구조적으로 선형의존성이 높기 때문에 페이지 쉬프트를 장착해서 출력 수열간의 상관관계를 낮춘다. 다음 정리는 행렬 H 가 기준수열에 대해 L 이상의 위상이동차를 갖게 하는 페이지 쉬프트가 됨을 보인다.

<정리1[9]> 상태전이행렬 M 을 갖는 n 셀 LFSR이 B 이하의 탭 수와 연속적인 상태전이를 통해 얻은 연속된 열의 위상이동차가 L 이상 되게 하는 페이지 쉬프트는 다음의 $n \times n$ 행렬 H 이다.

$$H = \begin{bmatrix} h_{p_0} \\ h_{p_1} \\ \vdots \\ h_{p_{n-1}} \end{bmatrix}$$

여기에서 $h_{p_i} = x_0 M^{p_i}$ ($0 \leq i \leq n-1$), $p_0 = 0$, $x_0 = (100 \dots 0)$, $p_i - p_{i-1} \geq L$, $|h_{p_i}| \leq B$ 이다. 또한 p_i 는 1열과 $i+1$ 열 사이의 위상이동차이고, $|h_{p_i}|$ 는 h_{p_i} 의 탭 수이다. 즉, H 는 p_0, p_1, \dots, p_{n-1} 을 위상이동차로 갖는 페이지 쉬프트이다. □

n 차 원시다항식 $c(x) = x^n + c_{n-1}x^{n-1} + \dots + c_1x + 1$ 를 특성다항식으로 갖는 LFSR에 대해서 페이지 쉬프트의 탭 수는 B 이하, 연속된 열의 위상이동차는 L 이상이 되도록 하는 H 를 찾는 새로운 방법을 제안한다. 먼저 외부 XOR LFSR의 동반행렬 M_{ex} 은 다음과 같다.

$$M_{ex} = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 \\ 1 & c_1 & c_2 & \dots & c_{n-2} & c_{n-1} \end{bmatrix}$$

본 논문에서는 외부 XOR LFSR에 대하여 다루고 있으므로 M_{ex} 를 간단히 M 이라 쓴다. 특성다항식 $c(x)$ 를 이용하여 $M^L = c_n M^{n-1} + \dots + c_1 M + d_0 I$ ($c_i \in \{0, 1\}$, $0 \leq i \leq n-1$)로 나타낼 수 있다. 여기서 I 는 n 차 단위행렬이다. M^L 을 구하기 위해 $x_0 = (100 \dots 0)$ 라 두면 다음을 만족한다.

$$M^L = \begin{bmatrix} x_0 M^L \\ x_0 M^B \\ \vdots \\ x_0 M^{n+1} \end{bmatrix}, M^B = \begin{bmatrix} x_0 M^B \\ x_0 M^A \\ \vdots \\ x_0 M^{n+2} \end{bmatrix}, \dots, M^{n-1} = \begin{bmatrix} x_0 M^{n-1} \\ x_0 M^n \\ \vdots \\ x_0 M^{2n-2} \end{bmatrix}$$

따라서 행렬의 곱셈을 하지 않더라도 초기값 $x_0 = (100 \dots 0)$ 를 $2n-2$ 번의 상태전이를 통해 M^L, M^B, \dots, M^{n-1} 을 얻을 수 있고 이것으로 M^L 을 쉽게 구할 수 있다.

<예제1> $c(x) = x^5 + x^2 + 1$ 을 특성다항식으로 하는 외부 XOR LFSR에 대한 전이행렬은 다음과 같다.

$$M = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \end{bmatrix}$$

특성다항식에 의해 $M^6 = M^2 + I$ 이고 $M^7 = M^4 + M^2$ 이다. 상태벡터 $X_0 = (10000)$ 을 8번 상태전이 시키면 $x_1 = (01000)$, $x_2 = (00100)$, $x_3 = (00010)$, $x_4 = (00001)$, $x_5 = (10100)$, $x_6 = (01010)$, $x_7 = (00101)$, $x_8 = (10110)$

$$\text{이므로 } M^2 = \begin{bmatrix} x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \end{bmatrix}, M^4 = \begin{bmatrix} x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix} \text{ 이고}$$

$$M^7 = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \end{bmatrix} \text{ 이다.} \quad \square$$

그림2는 32차 원시다항식을 특성다항식으로 갖는 32비트 LFSR의 상태전이를 나타낸 것이다. LFSR₅, LFSR₇, LFSR₉의 특성다항식은 다음과 같다. 여기서 LFSR₃는 항의 수가 5개인 32비트 LFSR을 의미한다.

- LFSR₅: $x^{32} + x^{16} + x^7 + x^2 + 1$
- LFSR₇: $x^{32} + x^{10} + x^4 + x^3 + x^2 + x + 1$
- LFSR₉: $x^{32} + x^{30} + x^9 + x^5 + x^4 + x^3 + x^2 + x + 1$

여기서 LFSR은 구조적으로 선형의존성이 높아서 난수성이 낮은 패턴을 생성함을 확인할 수 있다. 이러한 LFSR의 구조적 약점 때문에 LFSR에 페이지 쉬프트를 장착하는 연구가 이루어졌다. 특히 Kagaris [9]는 선형유

한상태기계의 종류에 상관없이 사용할 수 있는 통합된 방법을 제시하였다.

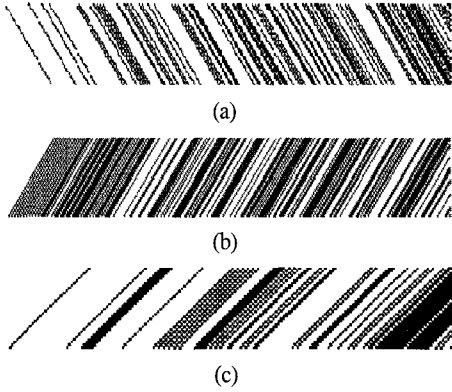


그림 2. 원시다항식을 특성다항식으로 갖는 32 bit LFSR의 상태 전이
(a) LFSR₅ (b) LFSR₇ (c) LFSR₉
Fig 2. State-transition of 32 bit LFSR whose characteristic polynomial is primitive
(a) LFSR₅ (b) LFSR₇ (c) LFSR₉

그러나 Kagaris의 방법을 LFSR에 적용함에 있어 선택된 벡터의 1의 갯수가 B 를 초과하면, 1단계씩 상태전이를 시키면서 생성되는 벡터가 원하는 조건을 충족시키는지 확인한다. 그러나 LFSR은 그림1과 같이 현재 상태에서 각 비트의 값들이 한 비트씩 이동되면서 다음 상태로 전이되기 때문에 조건을 충족하지 않는 벡터가 연이어 발생하게 된다. 그런데 표2에서 제안된 알고리즘에 따라 H 를 구성하면, Kagaris의 방법에 따라 H 를 구성하는 것보다 충족되지 않는 벡터를 선택하게 되는 단계를 효과적으로 줄일 수 있으므로 페이지 쉬프터를 훨씬 빨리 구성할 수 있다. 다음은 주어진 n 셀 LFSR에 대하여 위상이동차 L 과 탭수 B 가 주어질 때 H 를 구성하는 알고리즘이다.

<예제2> $c(x) = x^5 + x^2 + 1$ 를 특성다항식으로 갖는

외부 XOR LFSR에 대하여 $M = \begin{bmatrix} 01000 \\ 00100 \\ 00010 \\ 00001 \\ 10100 \end{bmatrix}$ 이다.

$B=2, L=7$ 을 만족하는 5×5 페이지 쉬프터 H 를 구성하

자. 먼저 예제1에 의해서 $M^T = \begin{bmatrix} 00101 \\ 10110 \\ 01011 \\ 10001 \\ 11100 \end{bmatrix}$ 이다. Step1에 의

해서 (10000)을 H 의 1행으로 둔다. Step2에 의해서 (10000) $M^T = (00101)$ 이다. 이것은 1의 수가 2 이하이고 H 에 이미 선택된 행이 아니므로 Step3에 의해서 H 의 2행으로 둔다. Step4에 의해서 Step2로 간다. Step2 의해서 (00101) $M^T = (10111)$ 이고 이것은 1의 수가 4 이므로 조건을 만족하지 않는다. 그러면 다시 Step2로 돌아가서 (10111) $M^T = (00011)$ 을 얻는다. 이는 주어진 조건을 만족하므로 3행으로 둔다. 이러한 방법으로 5행까지 구하면 7, 21, 4, 18번째 벡터가 사용되는 페이지 쉬프터

$$H = \begin{bmatrix} 10000 \\ 00101 \\ 00011 \\ 00001 \\ 11000 \end{bmatrix} \text{를 얻는다.} \quad \square$$

표 2. 페이지 쉬프터 H 구성 알고리즘
Table 2. Algorithm for the construction of phase shifter H

입력: B, L, M^L , 출력: H
Step1) 초기벡터 x_0 를 H 의 1행으로 둔다.
Step2) $x_0 = x_0 M^L$ 을 계산한다.
Step3) x_0 의 1의 수가 B 이하이고 H 에 이미 선택된 벡터가 아니면 H 의 다음 행으로 선택한다.
Step4) H 의 선택된 벡터수가 n 보다 작으면 Step2로 간다.

$x^5 + x^2 + 1$ 를 특성다항식으로 갖는 외부 XOR LFSR에 대하여 제안된 방법으로 구성된 페이지 쉬프터를 H_1 , Kagaris의 방법에 의해 7, 18, 29, 5번째 벡터로 구성된 페이지 쉬프터를 H_2 라 하면 H_1, H_2 는 다음과 같다.

$$H_1 = \begin{bmatrix} 10000 \\ 00101 \\ 00011 \\ 00001 \\ 11000 \end{bmatrix}, H_2 = \begin{bmatrix} 10000 \\ 00101 \\ 11000 \\ 10010 \\ 10100 \end{bmatrix}$$

표3에서 보는 것과 같이 H_1 에 의해서는 부적합벡터가 3번 발생하고, H_2 에 의해서는 부적합벡터가 8번 발생한다. 표3은 제안된 방법이 Kagaris의 방법과 비교하여 부적합벡터수가 적음을 보여준다.

IV. 실험결과 및 분석

LFSR은 기계적 특성상 각 셀의 출력 값이 시프트 되므로 phase shift 값이 1이 되어 선형 의존성이 매우 높다 (그림 2 참고). 그림 3은 제안한 방법에 의하여 LFSR₅, LFSR₇, LFSR₉에 탭수가 3이하이고 위상이동차가 3000 이상인 페이지 쉬프터를 적용한 상태 전이 그림이다. 여기서 검은 점은 셀의 상태=1이고, 흰 점은 셀의 상태=0임을 나타낸다. 이는 페이지 쉬프터에 의하여 각 출력 값의 선형 의존성이 낮아지고 상대적으로 난수성이 높아졌음을 알 수 있다.

표 3. 제안된 방법과 Kagaris의 방법 비교
Table 3. Comparison Kagaris's method with the proposed method

Cyc	$x_0^T M^i$	제안한 방법	Kagaris의 방법
0	10000	←1	←1
1	01000		
2	00100		
3	00010		
4	00001	←4	
5	10100		←5
6	01010		
7	00101	←2	←2
8	10110		
9	01011		
10	10001		
11	11100	부적합벡터3	
12	01110		
13	00111		
14	10111	부적합벡터1	부적합벡터1
15	11111		부적합벡터2
16	11011		부적합벡터3
17	11001		부적합벡터4
18	11000	←5	←3
19	01100		
20	00110		
21	00011	←3	
22	10101		
23	11110		
24	01111		
25	10011		부적합벡터5
26	11101		부적합벡터6
27	11010		부적합벡터7
28	01101	부적합벡터2	부적합벡터8
29	10010		←4
30	01001		

*←i : H의 i번째 행

*부적합벡터i : 1의 갯수가 B보다 큰 i번째 벡터

표 4는 그림 3의 LFSR5에 적용한 페이지 쉬프터 H의 구조와 이를 적용한 각 출력 값의 위상이동차이다. 여기서 두 번째 셀의 페이지 쉬프터 '7, 15, 27'은 2셀의 페이지 쉬프터가 7셀, 15셀, 27셀의 XOR에 의하여 구성됨을 의미하고, 2셀의 위상이동차는 1096893000이다.

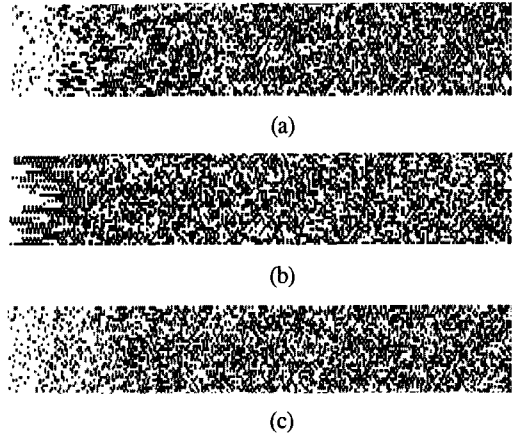


그림 3. 페이지 쉬프터를 적용한 32차 LFSR의 상태 전이
(a) phase shifter를 적용한 LFSR₅
(b) phase shifter를 적용한 LFSR₇
(c) phase shifter를 적용한 LFSR₉

Fig. 3. State-transitions of 32 bit LFSRs with phase shifters
(a) LFSR₅ with phase shifer
(b) LFSR₇ with phase shifer
(c) LFSR₉ with phase shifer

표 4. LFSR5의 페이지 쉬프터 H 구조
Table 4. Structure of phase shifter H of LFSR5

셀	phase shifter	위상이동차	셀	phase shifter	위상이동차
1	1	0	17	14,16,27	3492552000
2	7,15,27	1096893000	18	1,14,20	3620397000
3	4,12,31	2849598705	19	24,28	3685896000
4	9,11,26	310479000	20	4,16,17	439284000
5	3,13,22	2576064000	21	19,20,27	960474000
6	3,27,29	2614623705	22	9,14,19	446061000
7	20,24,25	2300739000	23	6	1208577000
8	8,30	1020054000	24	4,20,26	4135959705
9	8,10,16	10154637000	25	4,10,31	3951789000
10	6,10,20	1897272000	26	8,7,21	3502095000
11	6,23,29	2842941000	27	3,11,13	1178607705
12	7,22,25	3213621000	28	3,29,30	507144000
13	8,11,28	4250004000	29	23,28,32	1548459000
14	2,19,31	3293919000	30	1,24,28	1361271000
15	19,22,29	7262121000	31	7,20,32	3440094000
16	13,20,25	1833906000	32	18,27,28	1646001000

표 5는 탭수 $B=2$ 이고 위상이동차 $L=5$ 에 대하여 60개의 10차 원시다항식 중 5개의 10차 원시다항식을 갖는 LFSR에 페이지 쉬프터 H 를 구성할 때 부적합 벡터의 개수와 효율성을 나타낸 것이다.

여기서 원시다항식 10000101101은 $x^{10} + x^5 + x^3 + x^2 + 1$ 을 나타내고, N_1 과 N_2 는 각각 제안한 방법과 기존의 방법에 의하여 페이지 쉬프터 H 를 구성할 때 부적합 벡터가 발생하는 횟수이다. 즉 기존의 방법에 비하여 제안된 방법에 의해 H 를 구성하는 것이 시간이 적게 걸림을 알 수 있다. 효율성(E)는 $((N_2 - N_1)/N_2) \times 100(\%)$ 로 기존의 방법에 비하여 제안된 방법의 효율성을 나타낸다. $B=2$ 이고 $L=5$ 일 때 모든 10차 원시다항식에 대하여 60개의 LFSR에 페이지 쉬프터 H 를 구성할 때 부적합 벡터의 개수는 $40 \leq N_1 \leq 251, 193 \leq N_2 \leq 896$ 이며, 이에 대하여 효율성 E 는 $14.47 \leq E \leq 79.79$ 였다.

표 5. 부적합 벡터수와 효율성
Table 5. Number of unsuitable vectors and efficiency

원시다항식	N_1	N_2	E
10000101101	130	383	66.06
10001101111	195	228	14.47
10011100111	123	385	68.05
11011111101	156	772	79.79
10110001111	140	498	71.89

효율성을 그래프로 나타내면 그림 4와 같다. 그림 4에서 가로축은 60개의 원시다항식들이며 세로축은 각각 원시다항식에 대하여 계산된 효율성을 나타낸다. 이는 모든 경우에 대하여 효율성이 0보다 크다. 이는 제안된 방법이 기존의 방법보다 효율적임을 나타내는 것이다.

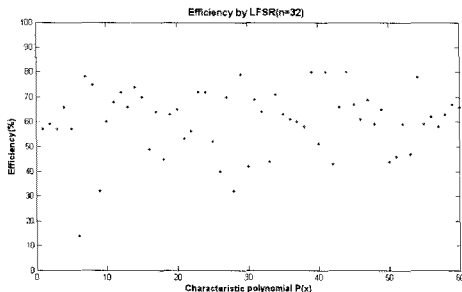


그림 4. 10비트 LFSR의 효율성
Fig. 4. Efficiency of 10 bit LFSR

그림 5는 $B=3$ 일 때 LFSR₅, LFSR₇, LFSR₉에 대하여 위상이동차 L 값이 500부터 5000까지 200씩 증가할 때의 효율성을 비교한 그래프이다. 여기서, 가로축은 L , 세로축은 효율성을 나타낸다. 그림에서 알 수 있듯이 항의 수가 적은 원시다항식을 갖는 LFSR에 대하여 제안된 방법이 기존의 방법보다 더 효율적임을 알 수 있다.

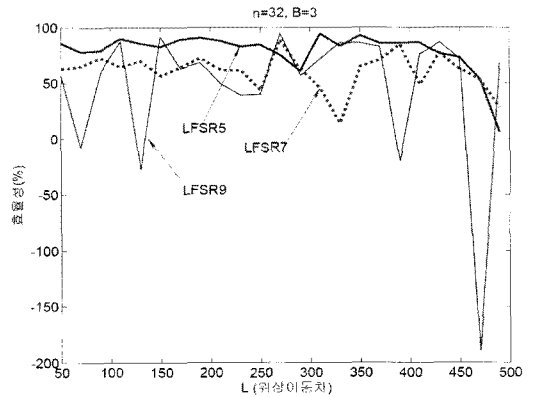


그림 5. L 의 변화에 따른 효율성
Fig. 5. Efficiency by L change

V. 결론 및 향후 연구방향

본 논문에서는 특성다항식을 원시다항식으로 갖는 LFSR을 사용하여 의사 난수 테스트 패턴을 생성하는데 있어 어떤 임의의 두 채널에서 출력되는 이진 수열의 선형의존성을 줄이기 위한 방법으로 적절한 탭 수를 유지하며 최소의 위상이동차를 보장하는 페이지 쉬프터를 갖는 LFSR 기반의 PRPG를 제안했다. 제안된 알고리즘에 따라 페이지 쉬프터를 구성하면, Kagaris의 방법에 따라 페이지 쉬프터를 구성하는 것보다 충족되지 않는 벡터를 선택하게 되는 단계를 효과적으로 줄일 수 있으므로 페이지 쉬프터를 훨씬 빨리 구성할 수 있는 장점이 있다.

참고문헌

[1] P.H. Bardell and W.H. McAnney, "Pseudo- random arrays for built-in tests," IEEE Trans. Comput., vol. C-35, no. 7, pp. 653-658, 1986.

[2] C. Dufaza and Y. Zorian, "On Some Theoretical Properties of LFSRs for BIST Applications," Proc. Int'l On-Line Testing Workshop, pp. 184-189, 1997.

[3] J. Rajski and J. Tyszer, "Design of phase shifters for BIST applications," in Proc. VLSI Test Symp., pp. 218-224, 1998.

[4] J. Rajski, N. Tamarapalli and J. Tyszer, "Automated Synthesis of Phase Shifters for Built-In Self-Test Applications," IEEE Trans. Computer-Aided Design, vol. 19, no. 10, pp. 1175-1188, 2000.

[5] K. Hatayama, M. Nakao, Y. Kiyoshige and K. Natsume, "Application of High-Quality Built-In Test to Industrial Designs," Proc. Int'l Test Conf., pp. 1003-1012, 2002.

[6] G. Mrugalski, J. Rajski and J. Tyszer, "Ring Generators-New Devices for Embedded Test Applications," IEEE Trans. Computer-Aided Design, vol. 23, no. 9, pp. 1306-1320, 2004.

[7] G. Mrugalski, J. Rajski and J. Tyszer, "High performance dense ring generators," Computers, IEEE Trans., vol. 55, no. 1, pp. 83-87, 2006.

[8] J. Kakade and D. Kagaris, "Phase shifts and linear dependencies," Circuits and Systems, ISCAS 2006. Proc. pp. 1595-1598, 2006.

[9] D. Kagaris, "A Unified Method for Phase Shifter Computation," ACM Trans. on Des. Auto. Electron. Syst., vol. 10, no. 1, pp. 157-167, 2005.

[10] J. Kakade and D. Kagaris, "Minimization of Linear Dependencies Through the Use of Phase Shifters," IEEE Trans. Computer-Aided Design of Int. Circuits and Systems, vol. 26, no. 10, pp. 1877-1882, 2007.

[11] P.H. Bardell, "Design Considerations for Parallel Pseudorandom Pattern Generators," J. Electronic Testing: Theory and Applications, vol. 1, no. 1, pp. 73-87, 1990.

저자소개



조성진 (Sung-Jin Cho)

1979년 2월: 강원대학교 수학교육과 학사
 1981년 2월: 고려대학교 수학과 석사
 1988년 2월: 고려대학교 수학과 박사
 1988년 ~ 현재: 부경대학교 응용수학과 정교수
 ※ 관심분야: 셀룰라 오토마타론, 정보보호, 부호이론, 컴퓨터 구조론



최연숙 (Un-Sook Choi)

1992년 2월: 성균관대학교 산업공학과 학사
 2000년 2월: 부경대학교 응용수학과 석사
 2004년 2월: 부경대학교 응용수학과 박사
 2004년 3월~2006년 2월: 영산대학교 자유전공학부 단임교수
 2006년 3월~현재: 동명대학교 미디어공학과 전임강사
 ※ 관심분야: 셀룰라 오토마타론, 정보보호, 부호이론, 컴퓨터 구조론



황윤희 (Yoon-Hee Hwang)

2002년 2월: 부경대학교 통계학과 학사
 2004년 2월: 부경대학교 응용수학과 석사
 2008년 8월: 부경대학교 정보보호학과 박사
 ※ 관심분야: 셀룰라 오토마타론, 정보보호, 유한체, 컴퓨터 구조론