

Skew Tent 맵에 비트 확장 기법을 적용하여 생성된 의사 혼돈 수열에 대한 분석

최효정, 김강산, *노홍준, 송홍엽

연세대학교, *LIG Nex1



목 차



I. 서론

II. 혼돈 맵과 LSB 확장 기법

- Tent 맵과 Skew Tent 맵
- 비트 확장 기법

III. 의사 혼돈 수열의 특성 분석

- 주기 분석
- 상관 특성 분석

IV. 결론

- 혼돈 맵은 미세한 초기값의 차이만으로 완전히 다른 실수 값이 도출되는 비선형 함수로 초기값의 변화만으로 주기가 없는 서로 다른 무한한 수열 생성 가능
 - 통신 시스템 및 이미지 암호화 등 여러 응용분야에서 활발한 연구 진행[1-5]
- 디지털 시스템에서 혼돈 수열을 구현하는 경우, 연산의 오차가 발생하여 동적저하 현상 발생
 - 혼돈 맵의 정의와 달리 짧은 주기성이 발생하거나 임의의 값으로 수렴함
- 디지털 구현 문제를 해결하기 위해 Tent 맵에 특정 비트를 확장하는 기법[2][3]이 제안됨.
- 본 논문에서는 Skew Tent 맵에 비트 확장 기법을 적용하여 생성된 의사 혼돈 수열의 주기성, 자기 상관 특성을 [2]의 결과와 비교하여 분석함

I. 서론

II. 혼돈 맵과 LSB 확장 기법

- Tent 맵과 Skew Tent 맵
- 비트 확장 기법

III. 의사 혼돈 수열의 특성 분석

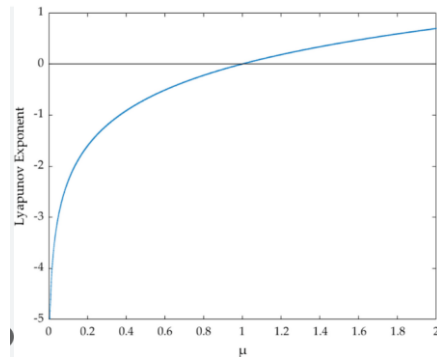
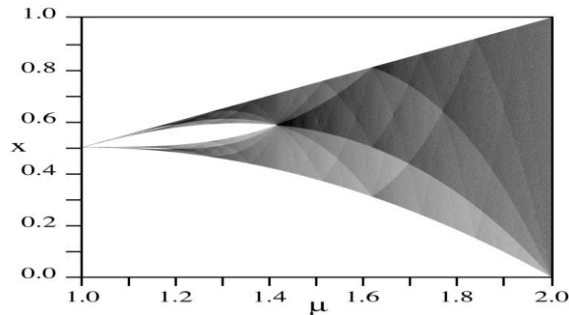
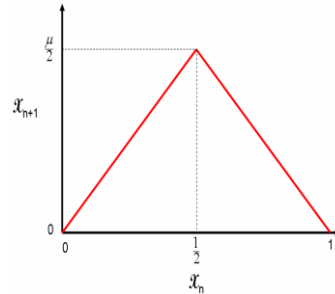
- 주기 분석
- 상관 특성 분석

IV. 결론

➤ Tent map

$$x_{n+1} = \begin{cases} \mu x_n, & 0 \leq x_n \leq 1/2 \\ \mu(1 - x_n), & 1/2 < x_n \leq 1 \end{cases}$$

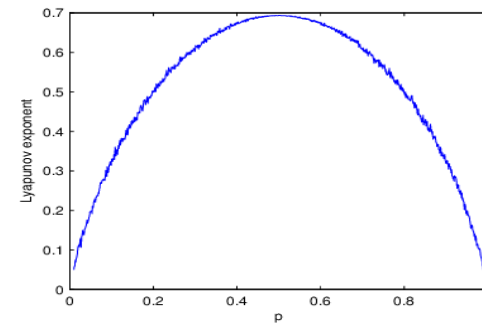
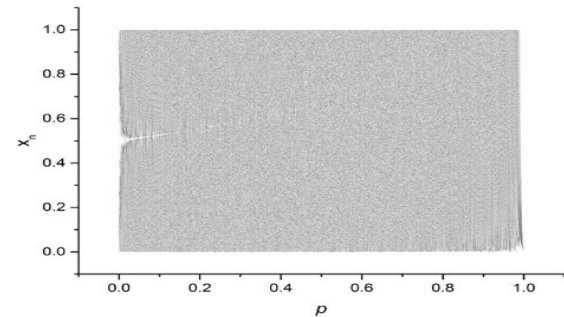
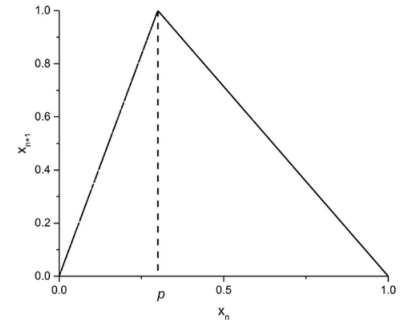
$$1 < \mu \leq 2$$



➤ Skew Tent map

$$x_{n+1} = \begin{cases} \frac{x_n}{p}, & 0 \leq x_n \leq p \\ \frac{1 - x_n}{1 - p}, & p < x_n \leq 1 \end{cases}$$

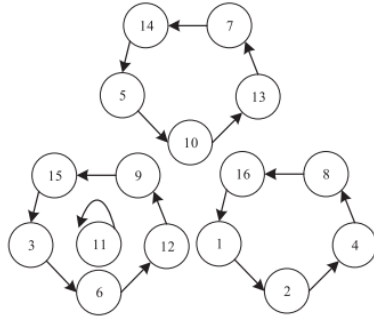
$$0 < p < 1$$



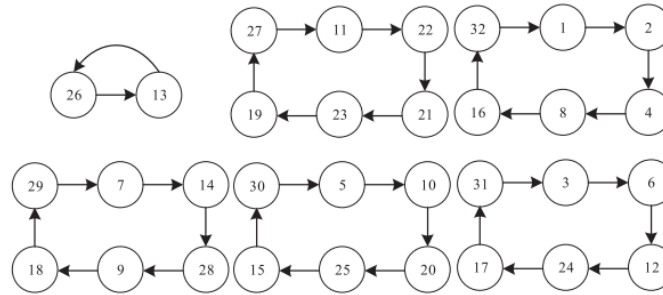
➤ Digital (integer) Skew-Tent map

$$x_{n+1} = \begin{cases} \frac{x_n}{p}, & 0 \leq x_n \leq p \\ \frac{1-x_n}{1-p}, & p < x_n \leq 1 \end{cases} \xrightarrow[\text{digital S.T.}]{[5]} z_{n+1} = \tilde{f}(z_n, a) = \begin{cases} \left\lfloor \frac{z_n \cdot 2^m}{a} \right\rfloor & 1 \leq z_n \leq a \\ \left\lfloor \frac{2^m \cdot (2^m - z_n)}{2^m - a} \right\rfloor + 1 & a < z_n \leq 2^m \end{cases}$$

$0 < p < 1, \quad x_n \in [0,1]$ $a \in (1, 2^m)$ $a = \lceil p \cdot 2^m \rceil$



(a) $m=4, p=8$



(b) $m=5, p=16$

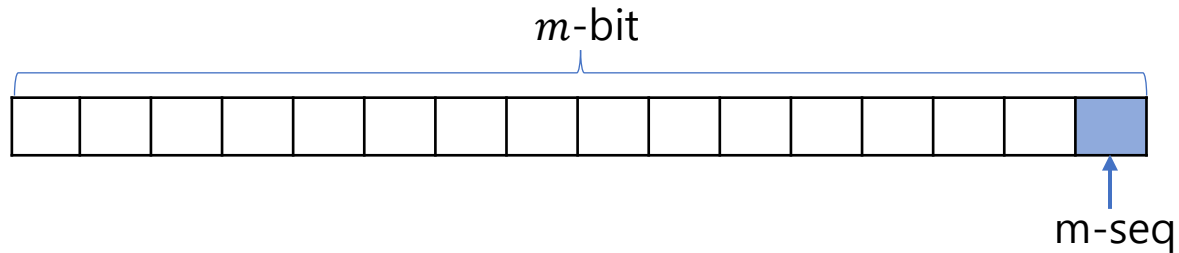


Skew-Tent map

➤ Digital (integer) Skew-Tent map

$$[5] \quad z_{n+1} = \tilde{f}(z_n, a) = \begin{cases} \left\lfloor \frac{z_n \cdot 2^m}{a} \right\rfloor & 1 \leq z_n \leq a \\ \left\lfloor \frac{2^m \cdot (2^m - z_n)}{2^m - a} \right\rfloor + 1 & a < z_n \leq 2^m \end{cases} \quad \begin{matrix} a \in (1, 2^m) \\ a = \lceil p \cdot 2^m \rceil \end{matrix}$$

↓ 식 변형



$$z_{n+1} = \begin{cases} \left\lfloor \frac{(z_n + 1)2^m}{a} \right\rfloor - 1, & 0 \leq z_n \leq a - 1 \\ \left\lfloor \frac{2^m(2^m - (z_n + 1))}{2^m - a} \right\rfloor, & a - 1 < z_n \leq 2^m - 1 \end{cases} \quad \begin{matrix} a \in (1, 2^m) \\ a = \lceil p \cdot 2^m \rceil \end{matrix}$$



기존 LSB 확장 기법[2]



➤ 이진 시프트 혼돈 맵에만 적용 가능

❖ 이진 시프트 혼돈 맵(Binary Shift Chaotic Map, BSCM)은 곱셈이 이진 시프트 연산이고, 덧셈 연산 중에 오버플로우가 발생하지 않는 혼돈 맵으로 정의

예) ■ Bernoulli map $S : [0, 1) \rightarrow [0, 1)$

$$S(x) = 2x \pmod{1} = \begin{cases} 2x, & 0 \leq x < 1/2 \\ 2x - 1, & 1/2 \leq x < 1 \end{cases}$$

Notice that S is just a left shift operation with discarding the most significant bit b_1 .

$$\text{i.e., } S(b_1 b_2 b_3 \dots)_2 = (b_2 b_3 b_4 \dots)_2$$

■ Tent map $T : [0,1) \rightarrow [0, 1)$

$$T(x) = \begin{cases} 2x, & 0 \leq x < 1/2 \\ 2(1-x), & 1/2 \leq x < 1 \end{cases}$$

기존 LSB 확장 기법[2]

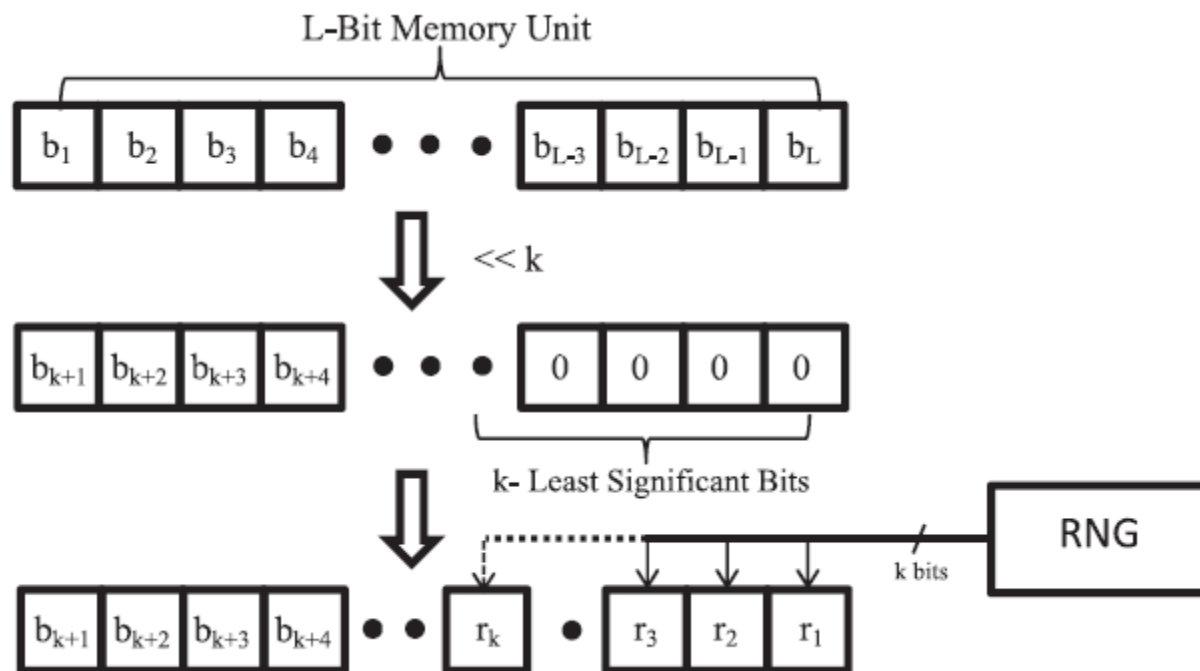
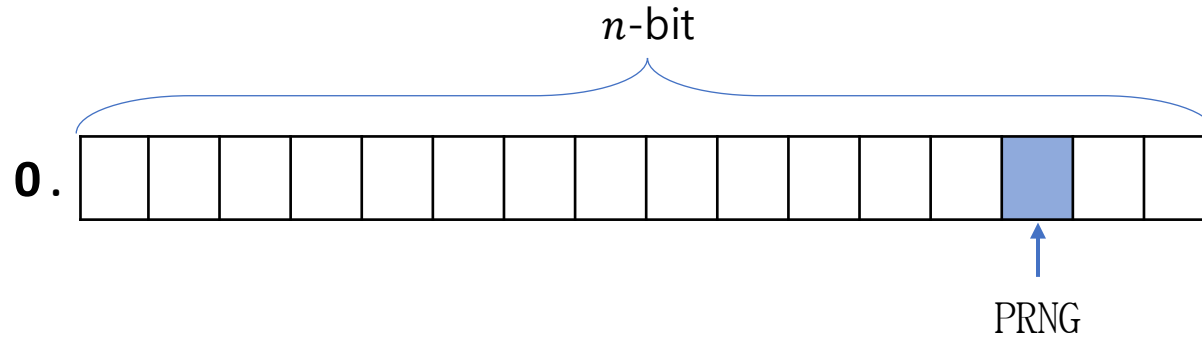


그림 1. LSB 확장 기법

- 간단하지만 다양한 fractal parameter를 사용할 수 없음



'Rounding Method' : 'Floor' – Round toward negative infinity.

- n -bit 고정소수점 연산
- 혼돈맵을 고정소수점 연산으로 계산 후 특정 비트를 PRNG로 확장
- 다양한 맵과 다양한 fractal parameter 적용 가능

I. 서론

II. 혼돈 맵과 LSB 확장 기법

- Tent 맵과 Skew Tent 맵
- 비트 확장 기법

III. 의사 혼돈 수열의 특성 분석

- 주기 분석
- 상관 특성 분석

IV. 결론

Skew-Tent map + LSB extension

➤ 기존 Tent map + Bit extension 방식 [3]



Tent map $g(x) = \begin{cases} \mu x, & 0 \leq x < 1/2 \\ \mu(1-x), & 1/2 \leq x \leq 1 \end{cases}$

$x^5 + x^2 + 1$

5bit

μ	확장 후 주기
1.03125	31
1.06250	31
1.09375	31
1.12500	31
1.15625	31
1.18750	31
1.21875	31, 93
1.25000	31, 62
1.28125	31, 62
1.31250	31, 62
1.34375	31
1.37500	31
1.40625	31
1.43750	31, 62
1.46875	31
1.50000	31

μ	확장 후 주기
1.53125	31
1.56250	31
1.59375	31
1.62500	31, 62
1.65625	31
1.68750	31
1.71875	31
1.75000	31
1.78125	31
1.81250	31
1.84375	31, 62
1.87500 (60)	31, 62, 93, 217 (=31*7)
1.90625 (61)	31, 62, 93, 217 (=31*7)
1.93750 (62)	31, 62, 93, 217 (=31*7)
1.96875 (63)	31, 62, 93, 217 (=31*7)
2.00000 (64)	31, 155 (=31*5)

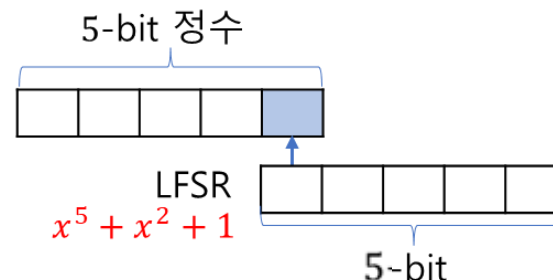
→ BSCM

Skew-Tent map + LSB extension

➤ Digital (integer) Skew-Tent + Bit extension 방식

$$z_{n+1} = \begin{cases} \left\lfloor \frac{(z_n + 1)2^m}{a} \right\rfloor - 1, & 0 \leq z_n \leq a - 1 \\ \left\lfloor \frac{2^m(2^m - (z_n + 1))}{2^m - a} \right\rfloor, & a - 1 < z_n \leq 2^m - 1 \end{cases}$$

5bit



a	확장 후 cycle	a	확장 후 cycle
2	31, 93, 186 (=31*6)	16	31, 155 (=31*5)
3	93, 124, 186 (=31*6)	17	31, 155 (=31*5)
4	31, 62, 310 (=31*10)	18	31, 62, 186, 217 (=31*7)
5	31, 465 (=31*15)	19	124, 372 (=31*12)
6	31, 434 (=31*14)	20	31, 465 (=31*15)
7	62, 93, 124, 217 (=31*7)	21	93, 403 (=31*13)
8	31, 93, 341 (=31*11)	22	31, 155 (=31*5) , 310 (=31*10)
9	31, 465 (=31*15)	23	217 (=31*7) , 279 (=31*9)
10	31, 155(=31*5), 279 (=31*9)	24	31, 93, 124, 248 (=31*8)
11	31, 93(=31*3), 341 (=31*11)	25	31, 403 (=31*13)
12	31, 62, 124, 186 (=31*6)	26	31, 155 (=31*5) , 279 (=31*9)
13	31, 62, 93, 310 (=31*10)	27	31, 155 (=31*5) , 279 (=31*9)
14	93, 310 (=31*10)	28	93, 403 (=31*13)
15	217, 279 (=31*9)	29	62, 93, 155, 186 (=31*6)

→ $\mu = 2$ 인 Tent map과 같은 경우

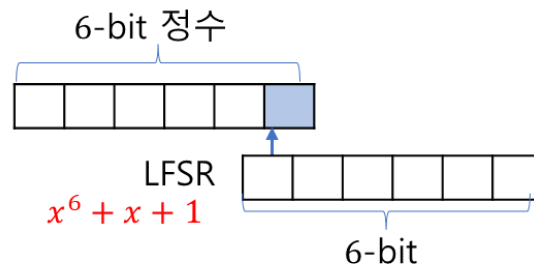
❖ 가능한 모든 a 값에 대해 주기가 크게 증가함

Skew-Tent map + LSB extension

➤ Digital (integer) Skew-Tent + Bit extension 방식

$$z_{n+1} = \begin{cases} \left\lfloor \frac{(z_n + 1)2^m}{a} \right\rfloor - 1, & 0 \leq z_n \leq a - 1 \\ \left\lfloor \frac{2^m(2^m - (z_n + 1))}{2^m - a} \right\rfloor, & a - 1 < z_n \leq 2^m - 1 \end{cases}$$

6bit



a	확장 후 cycle
2	63, 567(=63*9), 1197 (=63*19)
3	63, 126(=63*2), 1449 (=63*23)
4	63, 126, 189, 315(=63*5), 1071 (=63*17)
5	63, 126, 189, 1512 (=63*24)
6	63, 819, 1134 (=63*18)
7	63, 126, 1764 (=63*28)
8	63, 126, 756, 1071 (=63*17)
9	63, 126, 1575 (=63*25)
10	126, 189, 1575 (=63*25)
11	126, 252, 315, 1197 (=63*19)
12	63, 252, 819(=63*13), 882(=63*14)
13	63, 126, 252, 315, 1260(=63*20)
14	63, 126, 189, 630, 882(=63*14)
15	63, 126, 189, 1512(=63*24)

a	확장 후 cycle
16	63, 126, 189, 378, 1071 (=63*17)
17	63, 126, 189, 1449 (=63*23)
18	63, 567, 1197 (=63*19)
19	2016 (=63 * 32)
20	63, 315, 504, 1008(=63*16)
21	63, 126, 189, 378, 1260(=63*20)
22	126, 882, 1008(=63*16)
23	63, 567, 630, 756(=63*12)
24	63, 189, 693, 1071(=63*17)
25	63, 882, 1008(=63*16)
26	63, 441, 1323(=63*21)
27	441, 567, 1008 (=63*16)
28	63, 189, 1701 (=63*27)
29	63, 126, 252, 1512(=63*24)

❖ 가능한 모든 a 값에 대해 주기가 크게 증가함



Skew-Tent map + LSB extension

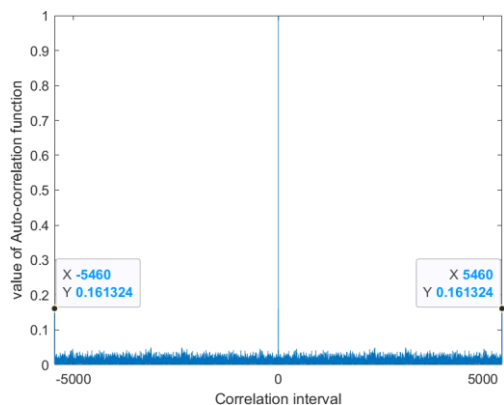


➤ S.T + LSB extension – Auto Correlation / Cross Correlation

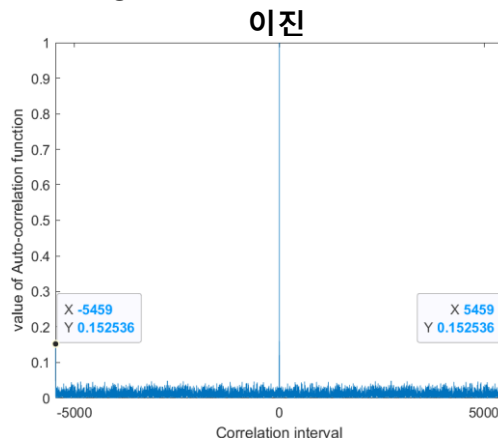
$$x^7 + x + 1$$

7bit S.-T. + 7bit LFSR ini = 0

$a = 55$
주기 5461
(127*43)



max : 0.1613
mean : 0.0114



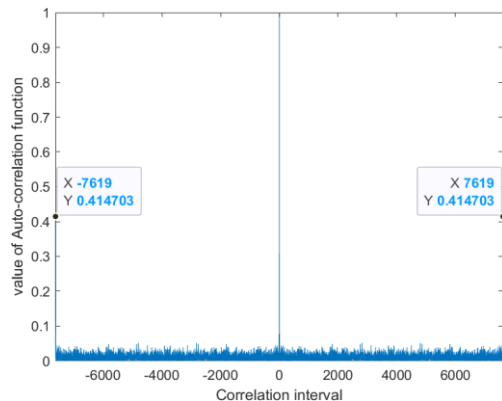
max : 0.1595
mean : 0.0118

Ab_Auto ✕

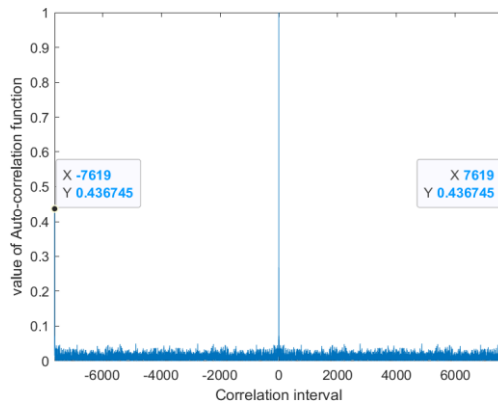
1x5461 double

1	2	3	4	5	...
1	0.1595	0.1525	0.1196	0.0489	...

$a = 92$
주기 7620
(127*60)



max : 0.4147
mean : 0.0114



max : 0.4367
mean : 0.0113

1	2	3	4	5	...
1	0.4367	0.0315	0.0304	0.0157	...

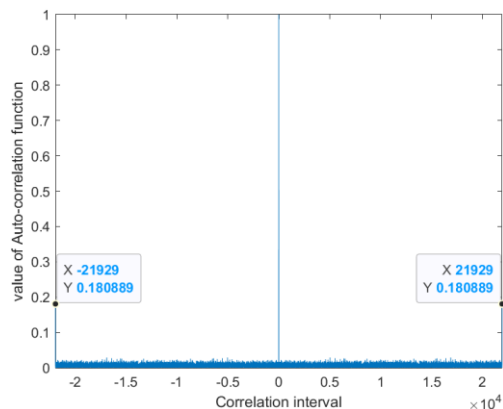
Skew-Tent map + LSB extension

➤ S.T + LSB extension – Auto Correlation / Cross Correlation

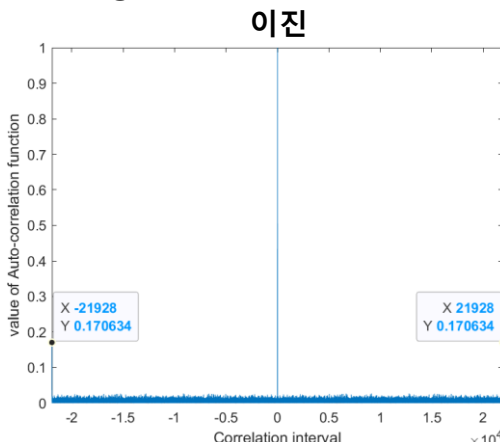
$$x^8 + x^4 + x^3 + x^2 + 1$$

8bit S.-T. + 8bit LFSR ini = 5

$a = 106$
주기 21930
(255***86**)



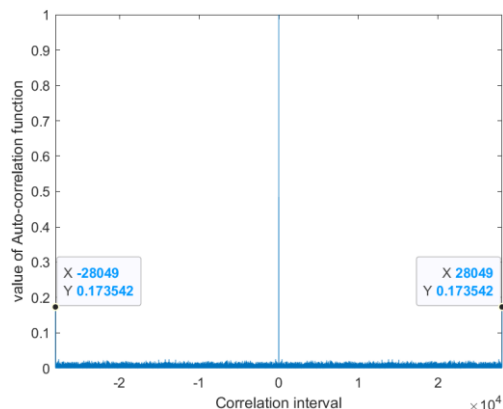
max : 0.1809
mean : 0.0057



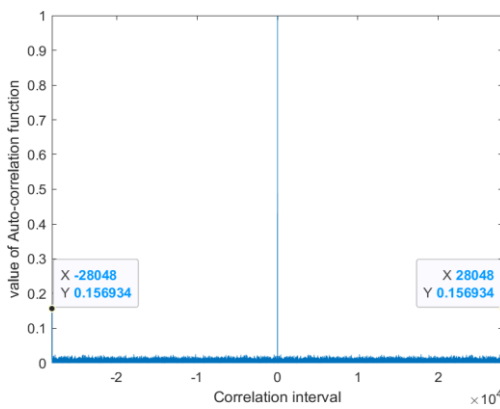
max : 0.1706
mean : 0.0060

Ab_Auto ✕					
1x21930 double					
1	2	3	4	5	...
1	0.1668	0.1706	0.1190	0.0643	...

$a = 107$
주기 28050
(255***110**)



max : 0.1735
mean : 0.0049



max : 0.1709
mean : 0.0052

Ab_Auto ✕					
1x28050 double					
1	2	3	4	5	...
1	0.1709	0.1569	0.1236	0.0735	...

➤ S.T + LSB extension – Auto Correlation / Cross Correlation

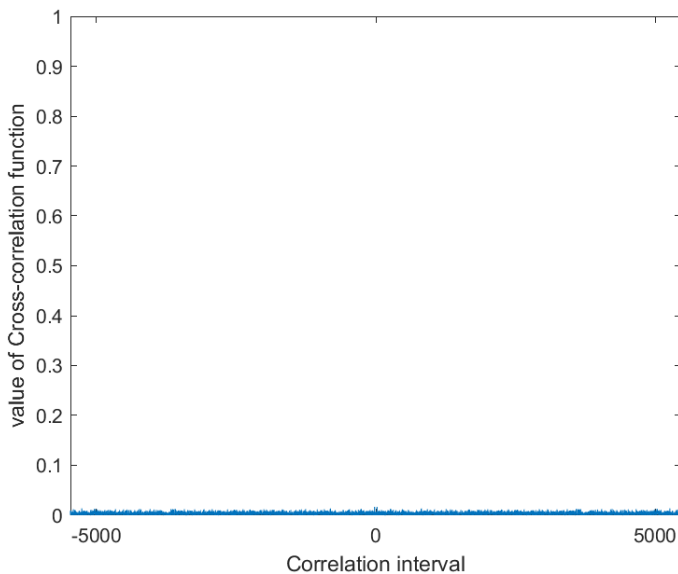
7bit S.-T. + 7bit LFSR ini = 0

$$x^7 + x + 1$$

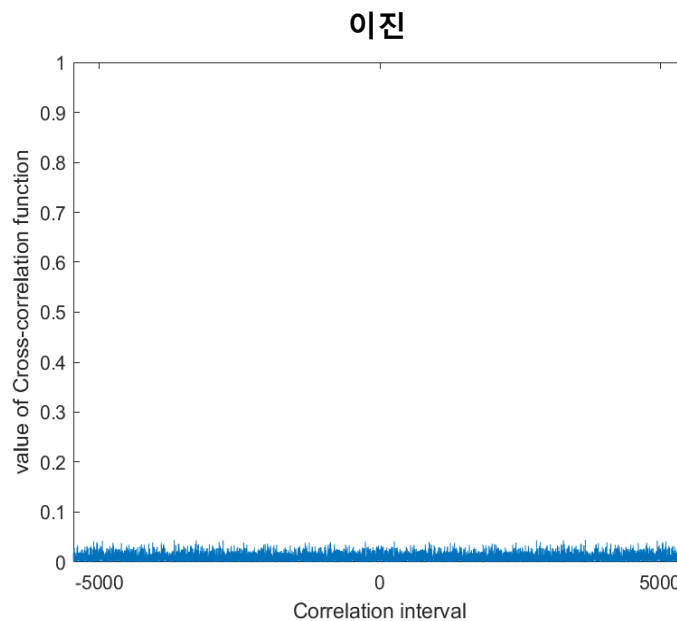
$a = 55$
주기 5461
(127*43)

$a = 92$
주기 7620
(127*60)

길이 5461로



max : 0.0168
mean : 0.0033



max : 0.0449
mean : 0.0100

a 값이 다른 수열들은 동일한 m-seq 사용해도 Cross-correlation 우수

➤ S.T + LSB extension – Auto Correlation / Cross Correlation

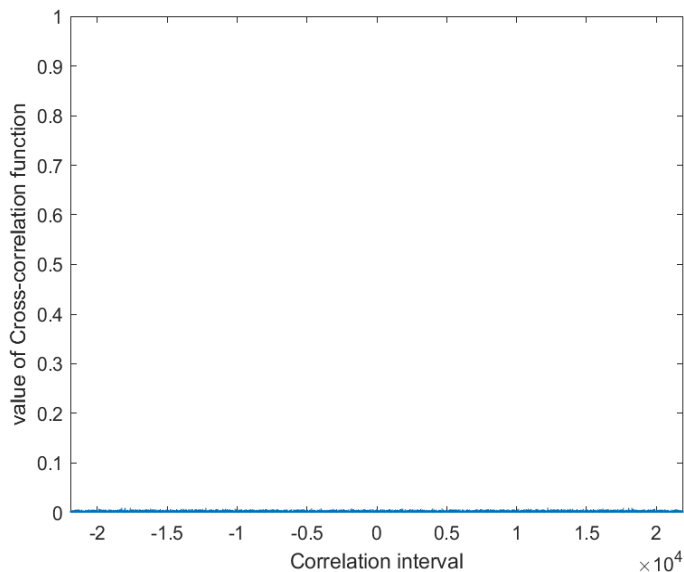
8bit S.-T. + 8bit LFSR ini = 5

$$x^8 + x^4 + x^3 + x^2 + 1$$

$a = 106$
주기 21930
(255***86**)

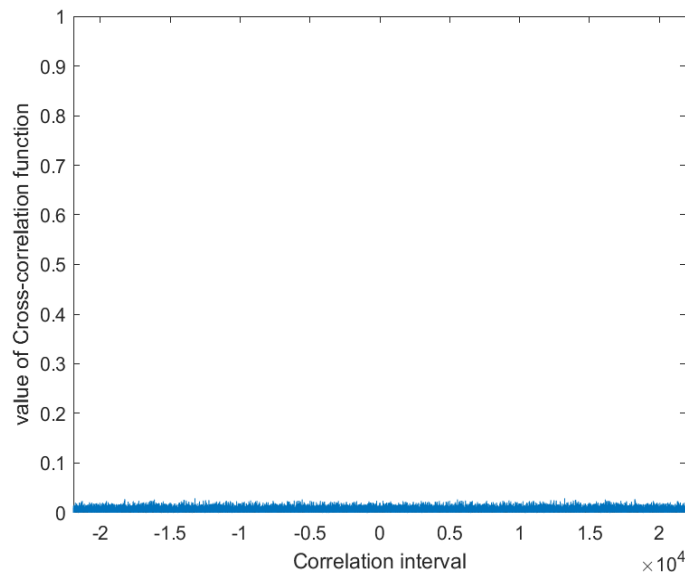
$a = 107$
주기 28050
(255***110**)

길이 21930으로



max : 0.0102
mean : 0.0019

이진



max : 0.0292
mean : 0.0058

a 값이 다른 수열들은 동일한 m-seq 사용해도 Cross-correlation 우수

I. 서론

II. 혼돈 맵과 LSB 확장 기법

- Tent 맵과 Skew Tent 맵
- 비트 확장 기법

III. 의사 혼돈 수열의 특성 분석

- 주기 분석
- 상관 특성 분석

IV. 결론

- 본 논문은 디지털 시스템에서 혼돈 맵을 구현할 때 발생하는 동적 저하를 개선하기 위해 혼돈 맵에 비트 확장 기법을 적용하여 출력된 수열의 주기성, 자기 상관 특성을 분석함

- 실험 결과
 - Tent 맵에 비트 확장 기법을 적용한 경우[3] 보다 Skew Tent 맵에 비트 확장 기법을 적용한 경우에 더 많은 파라미터에서 좋은 주기성을 가짐
 - Skew Tent 맵의 특성으로 인해 비트 확장 기법을 적용하였을 때 상호 상관 특성은 우수하지만 자기 상관 사이드로브에 피크값이 발생
 - 자기 상관 특성 개선을 위한 추가 연구 필요