이산화된 텐트맵의 설계

Design of Discretized Tent Map

백승재, 박진수
청주대학교 전자정보공학부

Seung-Jae Baek(bsj3386@empal.com), Jin-Soo Park(parkjs@cju.ac.kr)

요약

본 논문에서는 혼돈함수들 중 하나인 텐트함수의 변환을 수행하는 이산화된 8비트 텐트맵의 설계 절차를 보이기 위해서, 먼저 이산화 텐트맵의 진리표를 작성하였고, 진리표를 통해 구해진 간략화된 부울대수에 따라, 배타적 논리합 게이트만을 사용하여 이산화 맵을 실제 하드웨어로 구현하였다. 제안된 텐트맵 회로는 혼돈맵의 혼돈 특성에 따라 8비트 유한 정밀도와 주기 8의 상태들을 발생시키는 궤환회로로 구성되었으며, 설계된 회로도를 제시하였다. 이산화된 텐트맵은 스트림 암호시스템의 키스트림 발생회로에서 혼돈 2진 순서들을 발생시키는데 새롭게 사용될 것이다.

■ 중심어 : | 이산화텐트맵 | 난수성2진수 | 2진순서발생기 |

Abstract

To present the design procedure of discretized 8-bit tent map executing the transformation of tent function which is one of the chaotic functions, first, the truth table of discretized tent map was written, and then according to the simplified Boolean algebra equations obtained from the truth table, the discretized map is implemented with the exclusive logic gate as a real hardware.

The discretized tent map circuit which provides the feedback circuit for generating the period-8 states relevant to the 8-bit finite precision is also designed and presented in this paper. Furthermore, it might be used stream cipher system with a new key-stream circuit for generate of chaotic binary sequence.

■ keyword : | Discretized Tent Map | Random Binary | Binary Sequence Generator |

I. 서 론

본 논문에서는 스트림 암호시스템에서 가장 중요한 난수성(혼돈) 2진 키스트림 발생회로로 활용하고자 이산화된 텐트맵을 하드웨어로 구현하였다. 대표적인 1차원의 혼돈맵 (one dimensional chaotic map)들인, 톱니맵(saw-tooth map)과 텐트맵(tent map), 두 가지 중에서 톱니맵에 비해 약간 더 까다로운 텐트맵에 관한 이산화된 8비트 텐트맵의 설계 절차를 제시하였다. 이산화된 텐트맵(discritized tent map)은 스트림암호시스템(stream cipher system)의 핵심인 키스트림(Key-stream) 발생회로에서 혼돈 2진 순서들을 발생시키는데 새롭게 사용될 것이다[11].

기존의 연구로는 간략화된 부울식을 구하지 않고 프로그램 입력이 용이한, 효율성과 경제성이 떨어지는 롬 방식에 불과하며[12], 프로그램에 의한 소프트웨어적인

접수번호 : #080320-001
접수일자 : 2008년 03월 20일
심사완료일 : 2008년 04월 18일
교신저자 : 백승재, e-mail : bsj3386@empal.com

처리[11]가 아닌 간략화된 부울대수식에 의한 가장 효율적이고 최적화된 회로를 구성하기 위해서 부울함수를 사용한 하드웨어적인 접근은 본 연구가 처음이다.

8비트의 유한정밀도(finite precision)로 이산화된 텐트맵의 초기입력으로 8비트의 상태벡터(state vector)를 임의로 선정하였고, 이 논문에서는 초기입력 상태벡터로써 상태(10100100)을 사용하였다. 그리고 입력되는 8자리의 2진 상태마다 이산화 텐트맵에 의해 주기 8인 혼돈 2진 상태들을 발생시킬 수 있도록, 텐트맵의 궤환회로(feedback circuit)에는 8비트 병렬이동레지스터(8bit parallel shift register)를 연결하였다. 간략화된 부울대수(simplified Boolean algebra)에 따라 설계된 이산화된 텐트맵의 실제 구현에는 참고문헌[8]과는 다르게 이 논문의 [그림 4]와 [그림 5] 오직 7개의 배타적 논리게이트 소자(Ex-OR logic device)만을 사용해서 간결하게 제작하였다.

본 논문의 구성으로, 2장에서는 텐트맵에 의한 진리표를 구하는 과정에 대하여 소개하였으며, 3장에서는 이산화된 텐트맵을 하드웨어로 설계하고 구현하는 절차에 대하여 기술하고, 혼돈상태표와 혼돈거동을 보임으로써 본 연구의 타당성을 증명하였다. 끝으로 4장에서는 결론을 맺었다.

II. 텐트맵에 관한 이산화된 진리표 작성

혼돈거동을 내보이는 텐트함수를 식 (1)에 의해 표현하고 있으며, 그 그래프를 [그림 1]에 보였다[1-3].

$$T(x)=\begin{cases}2x, & 0.0 \le x < 0.5 \\ 2(1-x), & 0.5 \le x \le 1.0\end{cases} \tag{1}$$

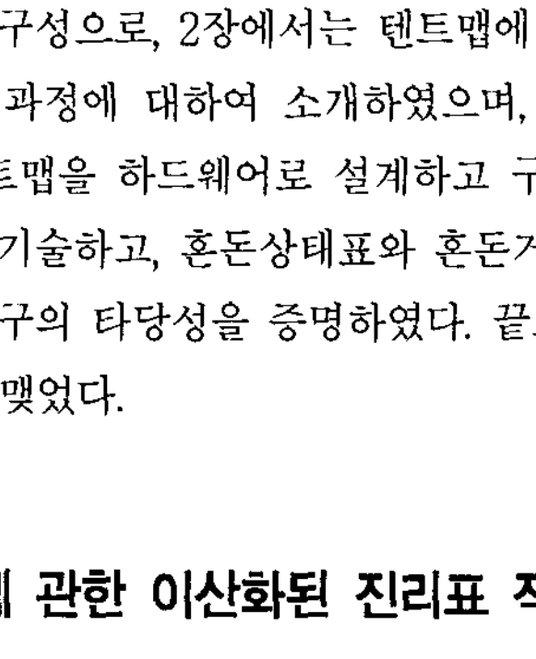

그림 1. 기울기 k=2인 텐트함수의 그래프(구간은(0,1])

텐트맵으로 사용하는 텐트함수는 구간 (0.5, 1.0]에서 수식표현이 $2-2x$인 관계로 톱니함수보다 까다로운 연산이 필요로 되는데, 그 결과는 이산화된 진리표에 관한 간략화된 부울함수(simplified Boolean function)의 배타적 논리합으로 나타났다.

텐트맵에 의한 한 번의 변환을 표현하는 식을 다음 형태로 정의하면 식 (1)보다 편리하다.

$$\begin{aligned} x_{n+1} &\equiv F[x_n] \\ &= (-1)^j \cdot \left[k \cdot x_n - 2 \cdot \left\lfloor \frac{j+1}{2} \right\rfloor\right] \end{aligned} \tag{2}$$

식 (2)에서 $j = \lfloor k \cdot x_n \rfloor$ 이며 $j = 0, 1, \cdots, k-1$은 부구간들의 수(the number of sub-interval)를 의미한다[4][5].

한편 텐트맵 $T(x)$는 기울기 $k = T'(x)$에 따라 [그림 2]처럼 구간의 길이를 변화시키고, 변환의 반복에 따른 임의의 근접한 두 점의 오차 ε는 다음 [그림 3]과 같이 전개되어 나타난다. 결국 반복의 횟수는 기울기의 거듭제곱과 같을 것이고,

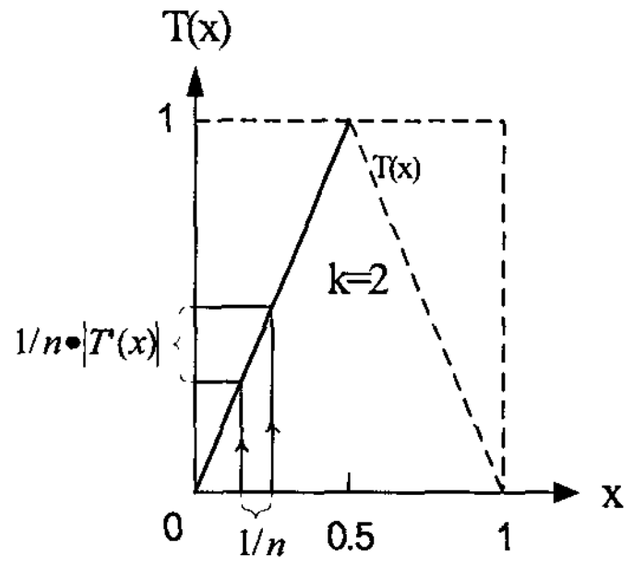

그림 2. 기울기와 한번의 $T(x)$ 변환에 따른 구간 길이 $1/n$의 변화

따라서 오차 ε는 기울기의 거듭제곱에 비례하여 식 (3)으로 정의되며, Liapunov지수 $\lambda(x_0)$은 기울기 k에 따르는 식 (3)에 의해

$$\left|\frac{d}{dx} T^n(x)\right| = 2n, \quad (n = 0, 1, 2, 3, \cdots) \tag{3}$$

결국 $\lambda(x_0)=\log 2$으로 정의한다[6].

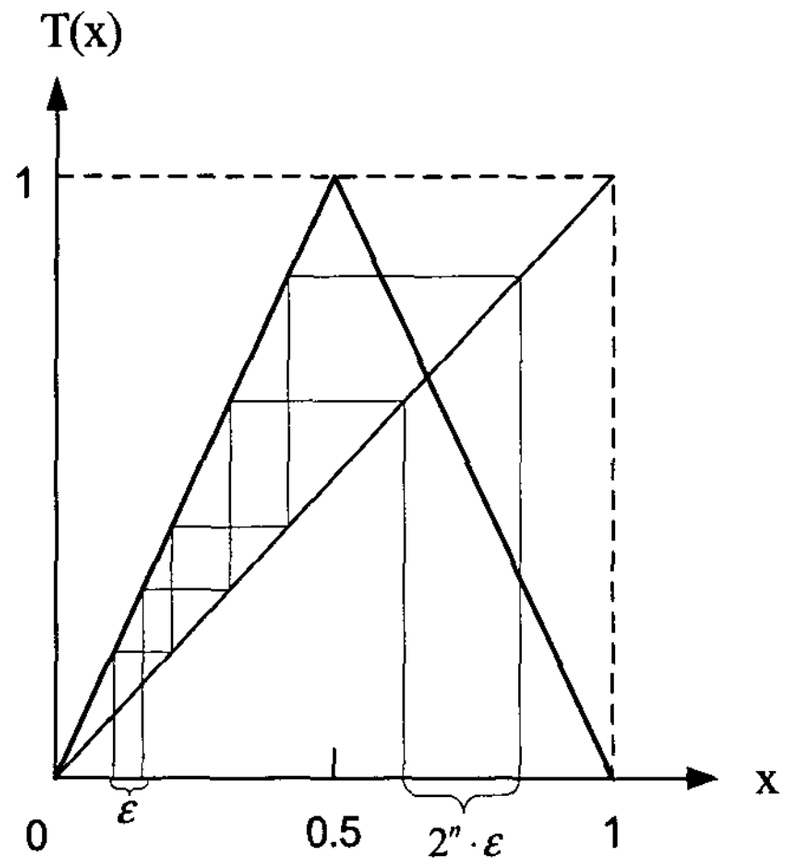

그림 3. 변환의 반복에 따른 오차 ε의 확장을 보여주는 그래프

작성한 텐트맵 구간 (0.0, 1.0]내에서의 진리표를 [표 1]에 보였다. 진리표의 입력변수는 255개의 8비트 상태변수를 나타내며 출력변수는 텐트함수를 8비트로 이산화하여 대응시킨 상태변수를 나타내었다.

표 1. 이산화 텐트맵에 관하여 부분적으로만 보인 진리표

	입력변수	출력변수
	$S_7S_6S_5S_4S_3S_2S_1S_0$	$C_7C_6C_5C_4C_3C_2C_1C_0$
1	00000001	00000010
2	00000010	00000100
3	00000011	00000110
4	00000100	00001000
5	00000101	00001010
6	00000110	00001100
7	00000111	00001110
8	00001000	00010000
9	00001001	00010010
10	00001010	00010100
⋮	⋮ ⋮	⋮ ⋮
126	01111110	11111100
127	01111111	11111110
128	10000000	11111111
129	10000001	11111101
130	10000010	11111011
131	10000011	11111001
132	10000100	11110111
133	10000101	11110101
134	10000110	11110011
135	10000111	11110001
⋮	⋮ ⋮	⋮ ⋮
246	11110110	00010011
247	11110111	00010001
248	11111000	00001111
249	11111001	00001101
250	11111010	00001011
251	11111011	00001001
252	11111100	00000111
253	11111101	00000101
254	11111110	00000011
255	11111111	00000001

III. 이산화된 텐트맵 회로의 설계와 구현

[표 1]에 보인 진리표로부터 입력변수에 대한 출력변수들에 관한 간략화된 부울함수는 식 (4)로 구해졌다.

$$C_0 = S_7, \quad C_1 = S_0 \oplus S_7,\ C_2 = S_1 \oplus S_7,$$
$$C_3 = S_2 \oplus S_7,\ C_4 = S_3 \oplus S_7,\ C_5 = S_4 \oplus S_7, \qquad (4)$$
$$C_6 = S_5 \oplus S_7,\ C_7 = S_6 \oplus S_7$$

구해진 간략화된 부울식을 사용하여 이산화된 8비트 텐트맵의 조합회로(combinational circuit)를 [그림 4]와 같이 설계하였고, 조합회로는 단지 배타적 논리게이트로 구성되며 게이트는 상태변수의 개수보다 1개 적은 7개이며, 입력변수 S_7은 출력변수 C_0로 직결되는 간단한 회로로 구성됨을 알 수 있다.

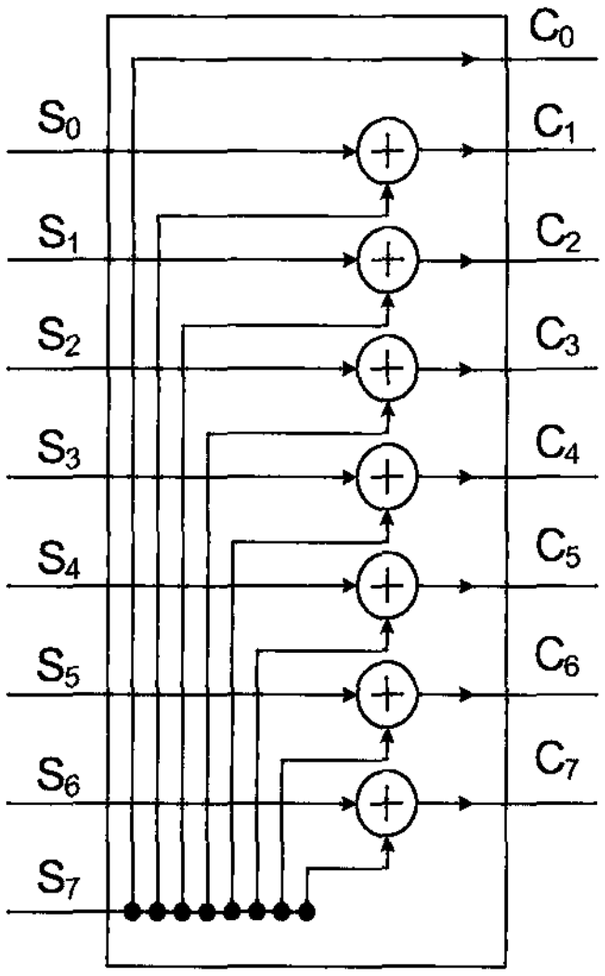

그림 4. 이산화된 텐트맵의 조합회로 설계

8비트의 상태 (10100100)를 초기 입력으로 주고, 주기 8인 혼돈상태들을 발생시키는 궤환회로를 갖는 이산화된 8비트 텐트맵 순차회로(sequential circuit)의 실제 구현을 [그림 5]에 나타내었다.

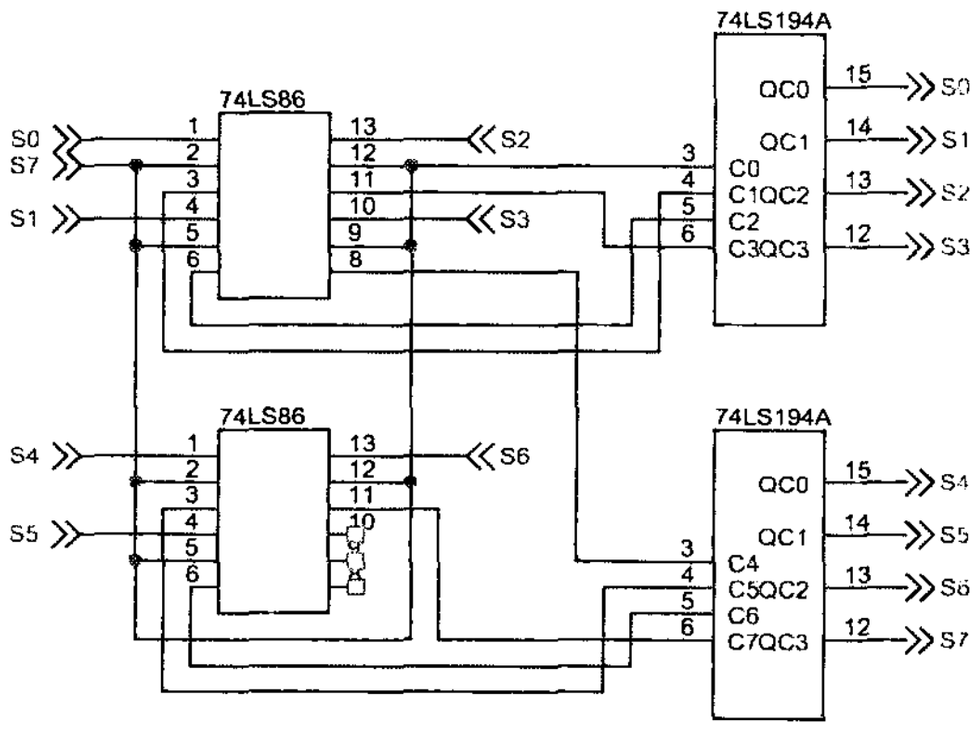

그림 5. 이산화된 8비트 텐트맵 회로의 실제구현

임의의 8비트 입력상태(10100100)에 의하여 주기 8을 가지며, 8가지의 혼돈상태들이 [표 2]와 같이 발생한다 [7].

표 1. 이산화 텐트맵 회로에서 발생하는 주기 8의 혼돈상태

	상태값	십진수
⓪	1 0 1 0 0 1 0 0	0.64062500
①	1 0 1 1 0 1 1 1	0.71484375
②	1 0 0 1 0 0 0 1	0.56640625
③	1 1 0 1 1 1 0 1	0.86328125
④	0 1 0 0 0 1 0 1	0.26953125
⑤	1 0 0 0 1 0 1 0	0.53906250
⑥	1 1 1 0 1 0 1 1	0.91796875
⑦	0 0 1 0 1 0 0 1	0.16015625
⑧	0 1 0 1 0 0 1 0	0.32031250
⑨	1 0 1 0 0 1 0 0	0.64062500

[표 2]의 8가지의 혼돈상태들을 텐트맵 상에 그래프로 나타내면 [그림 6]과 같은 주기성을 갖는 것을 확인할 수 있다. ⓪번째 상태값을 시점으로 주기 8이 되는 점 ⑨에서 종료됨을 알 수 있다. 그림에 표시된 원문자는 [표 2]의 십진수 값을 x축 상에 대응시킨 점을 의미한다.

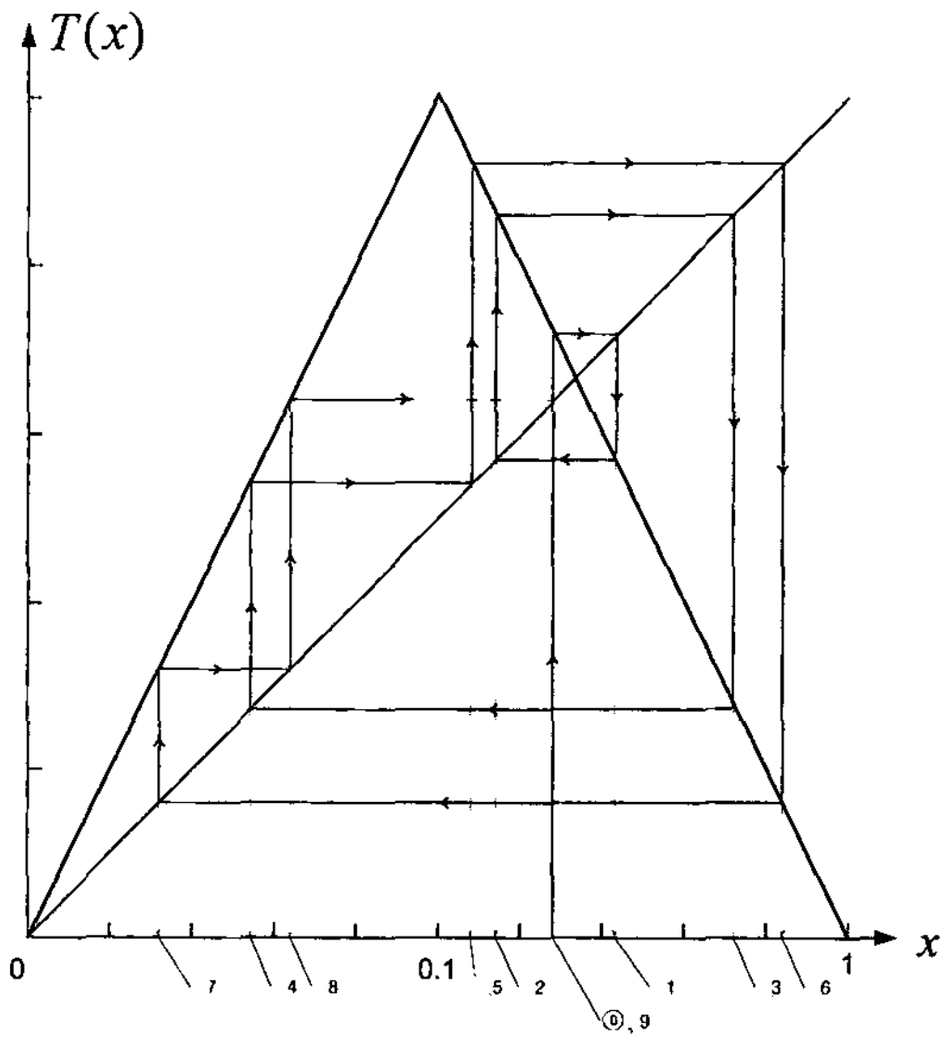

그림 6. 주기 8인 혼돈거동의 주기성

텐트맵 회로를 m-LFSR (maximum- length Linear Feedback Shift Registor)에 연결시켜 2진 순서를 발생하는데 사용한다면 주기 8인 혼돈상태에 의해 기존의

가장 이상적인 난수성 발생기인 mLFSR보다 8배 더 긴 주기를 갖게 됨을 알 수 있으며, 이로 인해 텐트맵을 연계한 난수발생기는 텐트맵의 혼돈특성을 나타낼 뿐만 아니라 그 혼돈주기에 의하여 더욱더 긴 난수주기를 가지게 되는 것이다.

IV. 결 론

이 논문에서는 이산화된 진리표[표 1]을 통해 간략화된 부울식(식 4)를 구한 후 [그림 4]와 같은 텐트맵의 설계를 통해 [그림 5]와 같은 실제회로를 구현하였고, [표 2]를 통해서 이산화된 텐트맵에서 발생하는 주기 8의 혼돈 상태를 발생시킬 수 있었다. 이산화된 텐트맵은 설계와 구현을 용이하게 하기위해 8비트만의 유한정밀도로 이산화 하였지만, 텐트맵의 이산화 진리표 작성과정과 작성된 진리표[표 1]로부터 얻어지는 출력변수들에 관한 부울함수식(식 4)을 통해 더 높은 유한정밀도를 갖도록 확대 설계하는 것도 비교적 수월하리라는 것을 유추할 수 있다. 또한 실제 구현 시 부딪히는 제작상의 다른 문제점도 없으리라는 것을 확신할 수 있다.

그간 발표된 논문들 [9][10]과는 다르게 이 논문에서는 이동레지스터와 배타적합 논리게이트, 이 두 종류의 기본적인 디지털소자만으로도 대표적인 1차원의 이산화된 8비트 텐트회로를 설계·제작할 수 있다는 것을 보였다. 또한 주기 8인 혼돈순서를 발생시킬 수 있다는 결과를 통해, 보다 높은 유한정밀도에 의해 발생하는 텐트맵이나 다른 혼돈맵의 혼돈출력 순서는 의심할 여지없이 혼돈성 혹은 난수성 특성을 갖게 될 것을 역시 확신할 수 있다. 또한 이산화 텐트맵 회로가 기존의 최대 길이의 난수성 2진 순서를 발생시키는 선형궤환이동레지스터(mLFSR)와 연접하여 사용한다면 보다 강하고 새로운 키스트림 발생회로로 제작할 수 있음을 확신할 수 있다.

참 고 문 헌

[1] Denny Gulick, *Encounters with Chaos*, University of Maryland collage park, McGrow-Hill, Inc., 1992.

[2] H. O. Peitgen, H.Jürgens, and D.Saupe, *Chaos and Fractals*, Springes-Verlag, 1992.

[3] J. Argyris, G.Faust, and M.Haase, *An exploration of chaos*, in Texts on Computaional Mathematics, NewYork, Elevier, Vol.7, Elsevier science B.V., 1994.

[4] M. Jessa, "Maximal cycle length of pseudo chaotic sequences generated by piece wise-linear maps", in proc. 50th int. symp. Circuits and Systems ISCAS'99, Vol.5, Orlando, FL, pp.450-453, FL, 1999.

[5] M. Jessa, "Correlation in pseudochaotic sequences generated in the set of natural numbers," in proc. 6th Int. Specialist Workshop on Nonlinear Dynamics of Electronics Systems NDES'98, Budapest, Hungary, pp.169-172, 1998.

[6] Heinz Georg Schuster, "Deterministic chaos," Weinhem, Germany, VCH Verlagstesellschaft, pp.24-27, 1989.

[7] M. Jessa "The Period of Sequences Generated by Tent-Like Maps," IEEE Trans, Circuits Syst.I, Vol.49, No.1, pp.84-89, 2002.

[8] 박광현, " 비선형 난수성 순서발생기의 설계", 충주대학교 논문집, 제40집, 제2호, pp.85-88, 2005(12).

[9] Alioto M, Bernardi S, Fort A, Rocchis, vignoli V, "Analysis and design of digital PRNGS based on the discretized saw-tooth map," proc. conf. Electron Circuits syst, Vol.2, pp.427-430, 2003.

[10] M. Jessa "Designing Security for Number Sequences Generated by Means of the Saw-tooth chatotic Map," IEEE Trans. Circuits Syst.I, Vol.53, No.5, pp.1140-1150, 2006.

[11] Chen g, Nao YB and Chui CK, "A symmetric image encryption scheme based on 3D chaotic

cat maps," Chaos, Solions&Fractals, Vol.12, pp.749-761, 2004.

[12] 박광현, "무리수 키를 사용하는 혼돈 맵의 2진 순서 발생기 구현", 충주대학교 논문집, 제42집, pp.315-319, 2007(12).

저 자 소 개

백 승 재(Seung-Jae Baek) 정회원

- 1997년 2월 : 청주대학교 전자공학과(공학사)
- 1999년 2월 : 청주대학교 전자공학과(공학석사)
- 1999년 2월 ~ 2002년 : 청주대학교 전자공학과(박사수료)
- 2004년~현재 : 한국폴리텍IV청주대학 정보통신홈네트워크과 IT교수

<관심분야> : 스트림암호, 부호이론, 정보이론, 디지털통신

박 진 수(Jin-Soo Park) 정회원

- 1975년 : 한양대학교 전자공학과(공학사)
- 1977년 : 한양대학교 전자통신과(공학석사)
- 1985년 : 한양대학교 전자통신과(공학박사)
- 1999년 ~ 2008년 2월 : RRC 정보통신연구센터 소장
- 1978년 ~ 현재 : 청주대학교 전자정보공학부 교수

<관심분야> : 이동통신, 디지털 통신, 부호이론, 스프레드스펙트럼, 스트림암호