한국항행학회 논문지 제17권 제3호 2013년 6월 (JKONI 17(3): 292-297, Jun. 2013)

혼돈 2진 스트림 발생기 설계

The Design of Chaotic Binary Tream Generator

서용원*, 박진수*

Yong-Won Seo*, Jin-Soo Park*

요 약

본 논문에서는 혼돈 스트림 발생기에 사용되는 혼돈합성함수의 디지털 회로설계를 연구 하였다. 혼돈키 스트림 발생기의 수학적 모델에 기인하는 전반적인 설계 개념과 절차를 자세히 설명하였다. 또한 혼돈 함수에 대한 이진화 2진 진리표를 보였다. 결과로서 1차원과 2차원 두 종류의 혼돈맵들-텐트맵과 삐뚤어진 로지스틱 맵-을 연결시켜 합성맵으로 사용하는 합성상태머신의 설계를 제시하였다.

Abstract

In this paper, The design of digital circuits for chaotic composition function which is used for the key-stream generator is studied in this work. The overall design concept and procedure due to the mathematical model of chaotic key-stream generator is to be the explained in detail, and also the discretized truth table of chaotic composition function is presented in this paper. consequently, a composition state machine based on the compositive map with connecting two types of one dimensional and two dimensional chaotic maps together is designed and presented.

Key words : Chaotic composition function, Tent function, Skewed logistic fuction, Key-stream generator.

I. 서 론

스트림 암호시스템(stream cipher system)의 성능과 안정성을 결정짓는 난수성 2진 스트림발생기의 설계에 혼돈역학을 내보이는 혼돈 함수들[1]을 수학적 모델, 즉 발생알고리즘으로 사용하였다.

이 논문에서는 스트림발생기에서 발생되는 일련의 2진 순서들의 난수성을 높이기 위한 방안으로써 1차원의 혼돈함수를 2차원의 혼돈함수의 변수로 사용하여 합성시킨 혼돈합성함수—1차원의 혼돈함수로는 텐트함수 $T_2(x)$를 사용하였고, 2차원의 혼돈함수로는 삐뚤어진 로지스틱 함수 $L_4(x)$를 사용하여 합성한 혼돈합성함수를 이용한 혼돈2진발생기, 즉 혼돈 2진 스트림 발생회로를 설계하였다[2],[3].

1차원 혼돈함수와 2차원 혼돈함수의 수학적 모델을 부울대수식을 얻기 위하여 각 함수를 변형되거나 삐뚤어진 형태로 변환하여 이산화 진리표를 작성하였다. 이산화 진리표를 이용하여 얻어진 간소화된 부울식을 이용하여 단순한 디지털조합회로를 설계하였다. 이 디지털 조합회로는 기존의 스트림발생기에 비해 빠른 속도와 보다 우수한 혼돈역학을 내포한다.

이 혼돈 2진 스트림 발생회로는 다음 그림 1에 보인 블럭도에서 비밀번호에 해당하는 키값에 의해 일련의 난수성 키스트림을 발생시키는 “난순성 2진 순

* 청주대학교 전자공학과(Department of Electronics Engineering, Cheongju University)
· 제1저자 (First Author) : 서용원(Yong-Won Seo, Tel : +82-43-218-8086, email : ds3dhy@hotmail.com)
· 접수일자 : 2013년 4월 18일 · 심사(수정)일자 : 2013년 4월 18일 (수정일자 : 2013년 6월 23일) · 게재일자 : 2013년 6월 30일
http://dx.doi.org/10.12673/jkoni.2013.17.3.292

서 발생기"부분이다.

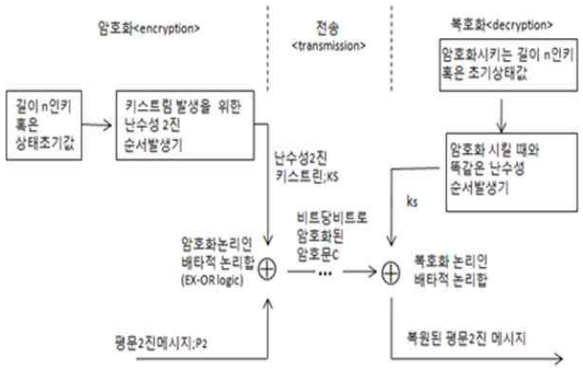


그림 1. 스트림 암호시스템의 블록도
Fig. 1. Block of stream cipher system

Ⅱ. 혼돈함수들의 이산화 진리표 작성과 디지털 회로설계

기존의 난수성 2진 발생기에 의해 난수성 2진 순서들을 발생시키기 위해서는, 초기의 2진 킷값을 궤환 함수(feedback function)에 해당하는 궤환 폐회로(closed feedback circuit)에 입력시키고, 선정한 비트 정밀도에 따라 멱승만큼 반복 통과시켜야 한다(예로, n-비트 정밀도의 초기 2진 킷값을 입력시킨다면, 궤환 폐회로를 2^n-1회 반복통과 시킴으로써 최대 2^n-1개의 난수성 2진 순서들을 얻게 된다)[4].

따라서 $L(T(x))$으로 표현되는 합성함수을 사용하여 난수성 2진 스트림 또는 혼돈 2진 순서들을 발생시키는 디지털 회로를 설계하기 위해서는 설계 절차에 따라 진리표을 작성해야 한다.

먼저 1차원의 혼돈함수인 텐트함수의 이산화된 텐트맵은 식 (1)으로 정의된다.

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

역시 십진수값 X = 0.0은 제외한 다음 표 1과 같이 이산화된 진리표에 의해 식 (7)과 같이 간략화 된 부울식을 구한 다음

표 1. 이산화 텐트맵의 진리표
Table 1. Truth table of discretized tent map

변수 / 순서	입력변수 I5	I4	I3	I2	I1	출력변수 T5	T4	T3	T2	T1
1	0	0	0	0	1	0	0	0	1	0
2	0	0	0	1	0	0	0	1	0	0
3	0	0	0	1	1	0	0	1	1	0
4	0	0	1	0	0	0	1	0	0	0
5	0	0	1	0	1	0	1	0	1	0
6	0	0	1	1	0	0	1	1	0	0
7	0	0	1	1	1	0	1	1	1	0
8	0	1	0	0	0	1	0	0	0	0
9	0	1	0	0	1	1	0	0	1	0
10	0	1	0	1	0	1	0	1	0	0
11	0	1	0	1	1	1	0	1	1	0
12	0	1	1	0	0	1	1	0	0	0
13	0	1	1	0	1	1	1	0	1	0
14	0	1	1	1	0	1	1	1	0	0
15	0	1	1	1	1	1	1	1	1	0
16	1	0	0	0	0	1	1	1	1	1
17	1	0	0	0	1	1	1	1	0	1
18	1	0	0	1	0	1	1	0	1	1
19	1	0	0	1	1	1	1	0	0	1
20	1	0	1	0	0	1	0	1	1	1
21	1	0	1	0	1	1	0	1	0	1
22	1	0	1	1	0	1	0	0	1	1
23	1	0	1	1	1	1	0	0	0	1
24	1	1	0	0	0	0	1	1	1	1
25	1	1	0	0	1	0	1	1	0	1
26	1	1	0	1	0	0	1	0	1	1
27	1	1	0	1	1	0	1	0	0	1
28	1	1	1	0	0	0	0	1	1	1
29	1	1	1	0	1	0	0	1	0	1
30	1	1	1	1	0	0	0	0	1	1
31	1	1	1	1	1	0	0	0	0	1

그림 2처럼 오직 배타적합논리게이트만을 사용하여, 간략화 된 부울식에 일치하는 선 연결만으로 설계 하였었다[5].

$$T_1=I_5,\ T_2=I_1\oplus I_5,\ T_3=I_2\oplus I_5, \quad (2)$$
$$T_4=I_3\oplus I_5,\ T_5=I_4\oplus I_5,$$

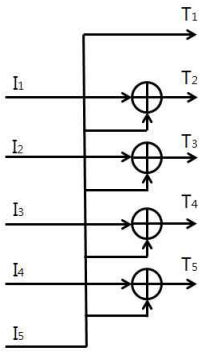


그림 2. 이산화된 텐트맵의 논리회로
Fig. 2. Logic circuit of discretized tent map

이어서, 2차원의 혼돈함수인 로지스틱 함수 $L_4(x)=4x(1-x)$에 관한 이산화 진리표는 5비트 정밀도의 한계를 극복하기 위하여, 변역값 $x(domain\ value)=0$을 제외한 단위 구간 $0<x\leq 1$내에서 다음 식(2)에 의하여 삐뚤어진 로지스틱 맵(skewed logistic map)의 형태로 변환시킨 다음 표 2와 같이 작성하였다.

$$L_4(x)=\sin^2\left[\frac{\pi\cdot T_2(x)}{2}\right] \tag{3}$$

식 (3)에서 $T_2(x)$는 기울기 $s=2$인 텐트함수(tent function)이므로 삐뚤어진 로지스틱 맵의 이산화된 값들은 텐트맵의 이산화 값들보다 조금씩 클 것이라는 것을 수식을 통해 유추할 수 있다[6],[7].

표 2에서도 표 1에서와 마찬가지로 첫 번째 이산순서(00000)는 제외되었고, 두 번째 이산순서(00001)와 함께 무정의 조건들로 사용하여 다음 부울식들(3)을 얻는다.

$$\begin{aligned}
L_1 &= \overline{I_2}\,\overline{I_3}\,\overline{I_4}\,\overline{I_5}+\overline{I_1},\\
L_2 &= \overline{I_2}\,\overline{I_3}\,\overline{I_5}+\overline{I_1}\,\overline{I_4}+\overline{I_1}\,\overline{I_4},\\
L_3 &= \overline{I_2}\,\overline{I_3}\,\overline{I_5}+\overline{I_1}\,\overline{I_3}\,\overline{I_4}+\overline{I_1}I_3I_4+I_1\overline{I_3}I_4+I_1I_3\overline{I_4},\\
L_4 &= \overline{I_1}\,\overline{I_3}\,\overline{I_4}I_5+I_1\overline{I_3}\,\overline{I_4}I_5+\overline{I_1}I_4I_5+\overline{I_1}I_3I_5+I_1I_4\overline{I_5}+I_1I_3\overline{I_5}+I_1\overline{I_2}\,\overline{I_5},\\
L_5 &= I
\end{aligned} \tag{4}$$

표 2. 삐뚤어진 로지스틱 맵 $L_{skewed}(x)$의 이산화 진리표
Tabel 2. Discretized truth table of skewed logistic map $L_{skewed}(x)$.

변수 / 순서	입력변수					출력변수				
	I_5	I_4	I_3	I_2	I_1	L_5	L_4	L_3	L_2	L_1
1	0	0	0	0	1	0	0	0	0	1
2	0	0	0	1	0	0	0	0	1	1
3	0	0	0	1	1	0	0	1	0	1
4	0	0	1	0	0	0	0	1	1	1
5	0	0	1	0	1	0	1	0	0	1
6	0	0	1	1	0	0	1	0	1	1
7	0	0	1	1	1	0	1	1	0	1
8	0	1	0	0	0	0	1	1	1	1
9	0	1	0	0	1	1	0	0	0	1
10	0	1	0	1	0	1	0	0	1	1
11	0	1	0	1	1	1	0	1	0	1
12	0	1	1	0	0	1	0	1	1	1
13	0	1	1	0	1	1	1	0	0	1
14	0	1	1	1	0	1	1	0	1	1
15	0	1	1	1	1	1	1	1	0	1
16	1	0	0	0	0	1	1	1	1	1
17	1	0	0	0	1	1	1	1	1	0
18	1	0	0	1	0	1	1	1	0	0
19	1	0	0	1	1	1	1	0	1	0
20	1	0	1	0	0	1	1	0	0	0
21	1	0	1	0	1	1	0	1	1	0
22	1	0	1	1	0	1	0	1	0	0
23	1	0	1	1	1	1	0	0	1	0
24	1	1	0	0	0	1	0	0	0	0
25	1	1	0	0	1	0	1	1	1	0
26	1	1	0	1	0	0	1	1	0	0
27	1	1	0	1	1	0	1	0	1	0
28	1	1	1	0	0	0	1	0	0	0
29	1	1	1	0	1	0	0	1	1	0
30	1	1	1	1	0	0	0	1	0	0
31	1	1	1	1	1	0	0	0	1	0

앞의 식(4)에 관한 디지털 회로 설계는 최소항의 곱논리를 구현하기 위한 21개의 AND gates와 5개의 출력변수에 관계하는 합논리를 구현하기 위한 5개의 OR gates, 그리고 기초적인 회로설계능력만을 필요로 하므로, 여기에서는 구체적인 회로설계 제시는 지면상 생략하며, 이후 디지털 회로의 표시는 다음 그림 3과 같이 블록으로 나타낸다.

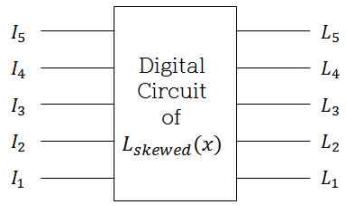


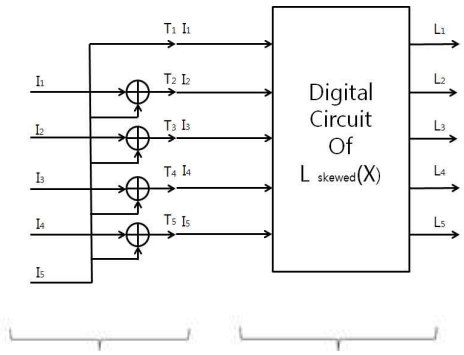
그림 3. 삐뚤어진 로지스틱 맵 $L_{skewed}(x)$ 의 회로.

Fig. 3. Circuit of skewed logistic map $L_{skewed}(x)$.

Ⅲ. 혼돈 합성함수의 이산화 진리표와 디지털 회로

혼돈합성함수 $L(S(x))$의 기능을 수행하는 합성맵에 관한 이산화 진리표는, 표 1에 보인 텐트맵 $T_2(x)$의 출력변수 값(T_5, T_4, T_3, T_2, T_1)을 합성맵의 입력 변수 값[표 2의 (I_5, I_4, I_3, I_2, I_1)]으로 사용하여 다음 표 3과 같이 작성한다.

표 3에 보인 " $T(x)$의 입력변수"와 $T(x)$의 출력변수이며 동시에 " $L(T(x))$의 입력변수"를 연결짓는 부울함수들은 식(1)로 구해졌고, " $L(T(x))$의 입력변수"와 " $L(T(x))$의 출력변수"에 관한 부울함수들도 이미 식 (3)으로 얻어졌으므로, 식 (1)과 식 (3)에 의해서 "삐뚤어진 혼돈합성 맵 $skewed\ \ L_4(T_2(x))$" 을 실현하는 디지털회로는 그림 3과 같이 설계된다.



텐트맵 $T_2(x)$의 회로 삐뚤어진 로지스틱 맵 $L_{skewed}(x)$ 회로

그림 4. 혼돈 합성맵 $L(T(x))$)의 회로.

Fig. 4. Circuit of chaotic composition map $L(T(x))$.

표 3. 혼돈 합성맵 $L(T(x))$의 이산화 진리표.

Table 3. Discretized truth table of chaotic composition map $L(T(x))$.

변수 / 순서	$T(x)$의 입력변수					$L(T(x))$의 입력변수					$L(T(x))$의 출력변수				
	I_5	I_4	I_3	I_2	I_1	T_5	T_4	T_3	T_2	T_1	L_5	L_4	L_3	L_2	L_1
1	0	0	0	0	1	0	0	0	1	0	0	0	0	1	1
2	0	0	0	1	0	0	0	1	0	0	0	0	1	1	1
3	0	0	0	1	1	0	0	1	1	0	0	1	0	1	1
4	0	0	1	0	0	0	1	0	0	0	0	1	1	1	1
5	0	0	1	0	1	0	1	0	1	0	1	0	0	1	1
6	0	0	1	1	0	0	1	1	0	0	1	0	1	1	1
7	0	0	1	1	1	0	1	1	1	0	1	1	0	1	1
8	0	1	0	0	0	1	0	0	0	0	1	1	1	1	1
9	0	1	0	0	1	1	0	0	1	0	1	1	1	0	0
10	0	1	0	1	0	1	0	1	0	0	1	1	0	0	0
11	0	1	0	1	1	1	0	1	1	0	1	0	1	0	0
12	0	1	1	0	0	1	1	0	0	0	1	0	0	0	0
13	0	1	1	0	1	1	1	0	1	0	0	1	1	0	0
14	0	1	1	1	0	1	1	1	0	0	0	1	0	0	0
15	0	1	1	1	1	1	1	1	1	0	0	0	1	0	0
16	1	0	0	0	0	1	1	1	1	1	0	0	0	0	1
17	1	0	0	0	1	1	1	1	0	1	0	0	1	0	1
18	1	0	0	1	0	1	1	0	1	1	0	1	0	0	1
19	1	0	0	1	1	1	1	0	0	1	0	1	1	0	1
20	1	0	1	0	0	1	0	1	1	1	1	0	0	0	1
21	1	0	1	0	1	1	0	1	0	1	1	0	1	0	1
22	1	0	1	1	0	1	0	0	1	1	1	1	0	0	1
23	1	0	1	1	1	1	0	0	0	1	1	1	1	0	1
24	1	1	0	0	0	0	1	1	1	1	1	1	1	1	0
25	1	1	0	0	1	0	1	1	0	1	1	1	0	1	0
26	1	1	0	1	0	0	1	0	1	1	1	0	1	1	0
27	1	1	0	1	1	0	1	0	0	1	1	0	0	1	0
28	1	1	1	0	0	0	0	1	1	1	0	1	1	1	0
29	1	1	1	0	1	0	0	1	0	1	0	1	0	1	0
30	1	1	1	1	0	0	0	0	1	1	0	0	1	1	0
31	1	1	1	1	1	0	0	0	0	1	0	0	0	1	0

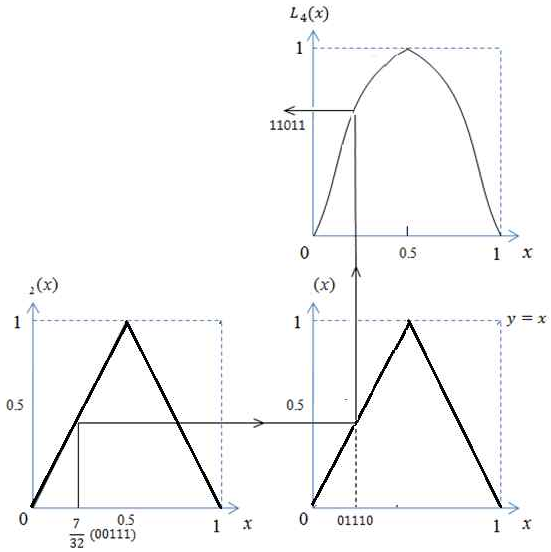


그림 5. 혼돈맵회로에서 수행되는 이산값(00111)의 변환 예

Fig. 5. Conversion example on the chaotic composition map using discretized binary value(00111)

그리고 그림 4의 디지털 회로에 의해 수행되는 혼돈의 움직임(chaotic dynamics)은 다음의 그림 5와 같고 발생된 출력변수값들(L_5, L_4, L_3, L_2, L_1)을 톱니맵의 입력변수값들(I_5, I_4, I_3, I_2, I_1)로 폐궤환회로(선)에 의해 반복 순환시킬 시에는, 길이가 제각각인 순환주기 10, 9, 6, 3, 2, 1 들을 갖는, 6개의 짧은 순환주기에 의해서 총 31개의 혼돈상태(순서)들을 발생시킨다는 것을 분석, 확인하였다.

Ⅴ. 결 론

이 논문에서 제시한 텐트함수와 로지스틱함수로 구성된 혼돈합성함수의 기능을 수행하는 혼돈 합성맵에 관한 디지털 회로의 경우, 입력되는 하나의 5비트 이산화된 키 값에 의해 5비트의 정밀도와 이산화 진리표의 이산값들의 순서에 기인하는 총 6개의 짧은 순환 주기가 발생하였다(이것은 5 bit라는 낮은 정밀도와 중복된 이산값의 발생에 기인했다).

이와 같은 문제점을 해결하는 방안으로는, 하나의 n비트 2진 킷값으로, 일련의 2^n-1개의 혼돈 2진 순서들을 모두 발생시킬 수 있도록 하기 위해서는, 혼돈 맵 회로의 출력측과 입력측을 연결하는 궤환 폐회로를 연결시키는 방법이 보다 효율적 이다는 것이 실험을 통해 도출되었다.

끝으로 혼돈 맵회로의 입력측에 선형 궤환 시프트 레지스터(LFSR)회로를 위치시킴으로써 총 $(2^n-1)\times(2^n-1)$개의 혼돈 2진 순서들을 발생시키는 혼돈 2진 키스트림 발생회로에 관한 디지털 회로설계가 가능하다.

Reference

[1] Heinz Georg Schuster, "Deterministic Chaos", *Weinhem Germany : VCH Verlagsgesellschaft.* pp. 24~27, 1989.

[2] Heinz-Otto, Peitgen,Hartmut Jürgens, and Dietmar Saupe, "Farctals for the Classroom", *Springer-verlag(NCTM)*, unit4, pp. 1~20, 1991.

[3] R.A.Rueppel, “Analysis and Design of Stream Cipher”, *Springer-Verlag, Berlin, Germany,* pp. 33~67, 1986.

[4] Solomon W. Golomb, “Shift Register Sequences”, *Aegean Park Press*, pp. 24~89, 1982.

[5] Kwang-Hyeon Park, Seung-Jae Baek, "Design of Random Binary Sequence Generator using the Chaotic Map", *Journal of the Korea Contents Association,* Vol.8, No.7, pp. 53~57, 2008.

[6] Kwang-Hyeon Park, “Design of the Logistic Map Based on the Tent Function”, *Journal of Chungju National University,* Vol.44, pp. 253~255, 2009.

[7] Yong-Won Seo, Jin-Soo Park, “Design of the Composition State Machine Based on the Chaotic Maps”, *Journal of the Korea Academia-Industrial cooperation Society,* Vol.10, No.12, pp. 3688-3693, 2009.

서 용 원 (Yong-Won Seo)

2002년 2월 : 청주대학교 전자공학과 (공학사)
2004년 2월 : 청주대학교 전자공학과 (공학석사)
2008년 9월 : 청주대학교 전자공학과 (박사수료)
2006년 ~ 현재 : (주)이씨엠 대표이사
관심분야 : 스트림암호, 부호이론, 정보이론, 디지털통신

박 진 수 (Jin-Soo Park)

1975년 : 한양대학교 전자공학과 (공학사)
1977년 : 한양대학교 전자통신과 (공학석사)
1985년 : 한양대학교 전자통신과 (공학박사)
1999년 ~ 2008. 2 : RRC 정보통신 연구센터 소장
1978년 ~ 현재 : 청주대학교 전자정보공학부 교수
관심분야 : 이동통신, 디지털 통신, 부호이론, 스프레드스펙트럼, 스트림암호