한국항행학회 논문지 제17권 제6호 2013년 12월 (JKONI 17(6): 652-657, Dec. 2013)

혼돈합성맵의 디지털회로설계

The design of digital circuit for chaotic composition map

박광현*, 서용원**

Kwang-Hyeon Park*, Yong-Won Seo**

요 약

논문에서는 두 가지 혼돈맵들을 연결시킨 하나의 합성맵을 기초로 사용하는 독립된 하나의 합성상태머신을 설계하는 방법 및 그 결과를 제시하였다. 혼돈2진스트림발생기로 사용하기 위하여 혼돈합성맵에 관한 디지털회로를 설계하였다. 두 가지 혼돈함수들- 톱니함수와 비뚤어진 로지스틱 함수-로 구성되는 혼돈합성함수의 이산화 진리표를 작성하였고, 디지털회로의 수학적 모델로써 간략화 된 부울대수식들을 제시하였다. 결과로써 혼돈합성함수의 맵에 관한 디지털회로들을 제시하였다.

Abstract

In this paper the design methode of a separated composition state machine based on the compositive map with two chaotic maps together and the result of that is proposed. The digital circuits of chaotic composition map for the use of chaotic binary stream generator are designed in this work. The discretized truth table of chaotic composition function which is composed of two chaotic functions - the saw tooth function and skewed logistic function - is made out, and also simplefied Boolean algebras of digital circuits are obtained as a mathematical model. Consequently, the digital circuits of the map for chaotic composition function are presented in this paper.

Key words : Saw-tooth and skewed logistic function, Chaotic composition function.

I. 서 론

스트림 암호시스템과 RSA암호로 대변되는 비대칭 암호시스템을 비교 하였을 경우, 스트림 암호시스템의 장점과 단점, 모두 다 난수성 2진 스트림 발생기에서 기인한다.

이러한 근본적인 특징을 갖고 있는 난수성 2진 스트림 암호시스템의 스트림 발생기에서 발생되는 일련의 2진 순서들의 난수성(randomness)을 높이기 위한 방안을 이 논문에서 연구하였다.

이를 위해 1차원의 혼돈함수를 2차원의 혼돈함수의 변수로 사용하여 합성시킨 혼돈합성함수(chaotic composition function)—1차원의 혼돈함수로는 톱니함수 (saw-tooth function)를 사용하고, 2차원의 혼돈함수로는 로지스틱 함수 (logistic function)를 사용하여 합성한 혼돈합성함수—의 기능을 수행하는 맵(map)에 관한 디지털 조합회로를 (digital combinational circuit) 설계하였다 [1], [2] ,[3].

디지털조합회로의 설계절차로는 혼돈합성맵에 관한 이산화 진리표(discretized truth table)를 작성하였고, 설계할 디지털 조합회로의 수학적모델(mathematical model)로써 간략화된 부울대수식들

* 한국교통대학교 정보통신공학과(Department of Information & Communications Engineering, Korea National University of Transportation)
** 청주대학교(Cheongju University)
· 제1저자 (First Author) : 박광현(Kwang-Hyeon Park, Tel : +82-43-218-8085, email : ds3dhy@hotmail.com)
· 접수일자 : 2013년 5월 13일 · 심사(수정)일자 : 2013년 5월 15일 (수정일자 : 2013년 12월 21일) · 게재일자 : 2013년 12월 30일
http://dx.doi.org/10.12673/jkoni.2013.17.6.652

(simplefied Boolean algebras)을 얻은 후에 회로를 구현하는 표준설계절차를 따랐다.

이렇게 설계된 혼돈2진 스트림 발생기는 단순한 발생 알고리즘에 의해 기존의 스트림 발생기에 비해서, 빠른 속도를 갖을 뿐아니라, 혼돈역학을 내포하므로 정보(혹은 평문의 메시지)를 보다 안전하게 암호화 할 수 있다.

Ⅱ. 톱니함수의 이산화 진리표 작성과 디지털조합 회로설계

기존의 2진 스트림 발생기(binaty stream generator)에서는 난수성 2진 순서들을 (randomness binary sequences) 발생시키기 위해 초기에 주어지는 2진 킷값(initial binary key-value)을 n-비트의 크기 또는 길이로 하였을 경우, 이 n-비트의 2진수를 궤환함수(feedback function)에 해당하는 궤환 폐회로(closed feedback circuit)에 입력시키고, 이 궤환 폐회로를 2^n-1회 반복통과 시킴으로써 최대 2^n-1개의 난수성 2진 순서들을 얻었다[4].

이와 같은 개념으로 $S_2(x)$으로 표현되는 톱니함수(saw-tooth function)를 수학적 모델로 사용하여 난수성 2진 스트림(rendomness binary stream) 또는 혼돈 2진 순서들(chaotic binary sequences)을 발생시키는 디지털 회로를 설계하기 위해서는 첫 번째로 톱니함수의 이산화진리표(discretized truth table)를 작성해야 한다.

따라서, 1차원의 혼돈함수이며, 기울기 $s=2$인 톱니함수 $S_2(x)$의 함수 기능을 수행할 5비트 정밀도(5-bit precision)를 갖는 톱니맵(saw-tooth map)에 관한 진리표로써 이산 2진 값들(discrete binary values)을 사용하여 표 1과 같은 이산화 진리표(discretized truth table)을 작성하였다.

이산화 진리표 1은 첫 번째 이산순서(00000)을 제외한 경우이며, 이 첫 번째 이산순서와 31번째 이산순서(11111)를 무정의 조건들(don't care conditions)로 사용하면, 이 진리표로부터 다음 식(1)들과 같은 간략화된 부울식을 얻을 수 있다.

$$S_1 = I_5, S_2 = I_1, S_3 = I_2, S_4 = I_3, S_5 = I_4 \qquad (1)$$

이 식 (1)에 의해 5비트의 톱니맵 기능을 실현하는 디지털 회로는 그림 1과 같이 설계 한다[5].

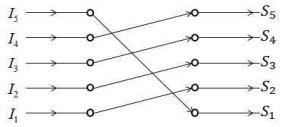

그림 1. 톱니맵 $S_2(x)$의 디지털 회로
Fig. 1. Digital circuit of saw-tooth map $S_2(x)$

표 1. 톱니맵 $S_2(x)$의 이산화 진리표
Table 1. Discretized truth table of saw-tooth map $S_2(x)$

변수 / 순서	입력변수					출력변수				
	I_5	I_4	I_3	I_2	I_1	S_5	S_4	S_3	S_2	S_1
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	0	0	0	0	1
17	1	0	0	0	1	0	0	0	1	1
18	1	0	0	1	0	0	0	1	0	1
19	1	0	0	1	1	0	0	1	1	1
20	1	0	1	0	0	0	1	0	0	1
21	1	0	1	0	1	0	1	0	1	1
22	1	0	1	1	0	0	1	1	0	1
23	1	0	1	1	1	0	1	1	1	1
24	1	1	0	0	0	1	0	0	0	1
25	1	1	0	0	1	1	0	0	1	1
26	1	1	0	1	0	1	0	1	0	1
27	1	1	0	1	1	1	0	1	1	1
28	1	1	1	0	0	1	1	0	0	1
29	1	1	1	0	1	1	1	0	1	1
30	1	1	1	1	0	1	1	1	0	1
31	1	1	1	1	1	1	1	1	1	1

이어서, 두 번째로 2차원의 혼돈함수인 로지스틱 함수 $L_4(x)=4x(1-x)$에 관한 이산화 진리표를 작성할 경우에서는, 5비트 정밀도에 따른 중복된 이산

2진값들의 출현을 배제하기 위하여, $x=0$ 을 제외한 단위 구간 $0<x\le 1$내에서, 다음 식(2)에 의한 로지스틱 맵(logistic map)의 형태, 즉 삐뚤어진 로지스틱 맵(skewed logistic map)의 형태로 변환시킨 후 다음 표 2와 같은 이산화 진리표를 작성하였다.

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

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

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

$$\begin{aligned}
L_1 &= \overline{I_2}\,\overline{I_3}\,\overline{I_4}\,\overline{I_5}+\overline{I_1}, \\
L_2 &= \overline{I_2}\,\overline{I_3}\,\overline{I_5}+\overline{I_1}\,\overline{I_4}+\overline{I_1}\,\overline{I_4}, \\
L_3 &= \overline{I_2}\,\overline{I_3}\,\overline{I_5}+\overline{I_1}\,\overline{I_3}\,\overline{I_4}+\overline{I_1}I_3I_4+I_1\overline{I_3}I_4+I_1I_3\overline{I_4}, \\
L_4 &= \overline{I_1}\,\overline{I_3}\,\overline{I_4}I_5+I_1\overline{I_3}\,\overline{I_4}I_5+\overline{I_1}I_4I_5+\overline{I_1}I_3I_5 \\
&\quad +I_1I_4\overline{I_5}+I_1I_3\overline{I_5}+I_1\overline{I_2}\,\overline{I_5}, \\
L_5 &= I
\end{aligned} \tag{3}$$

앞의 식(3)에 관한 디지털 회로 설계는 최소항(minterm)의 곱논리를 구현하기 위한 21개의 AND 논리게이트들(logic gates)과 5개의 출력변수에 관계하는 합논리를 구현하기 위한 5개의 OR 논리게이트들, 그리고 기초적인 2단계의 조합 회로설계능력만을 필요로 하므로, 여기에서 구체적인 회로설계 제시는 지면상 생략하며, 이후 디지털 회로의 표시는 다음 그림 2와 같이 블록으로 나타낸다.

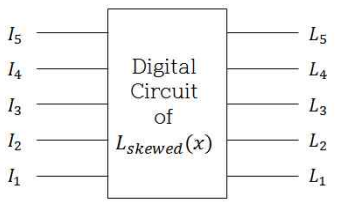

그림 2. 삐뚤어진 로지스틱 맵 $L_{skewed}(x)$ 의 블럭.
Fig. 2. Block of skewed logistic map $L_{skewed}(x)$.

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

Ⅲ. 혼돈 합성함수의 이산화 진리표와 디지털 회로

앞 절2. 에서 구한 톱니함수 $S_2(x)$와 삐뚤어진 $L_4(x)$의 이산화 진리표를 이용하는, 혼돈합성함수 $L(S(x))$의 기능을 수행하는 합성맵에 관한 이산화 진리표는, 표 1에 보인 톱니맵$S_2(x)$의 출력변수 값 (S_5, S_4, S_3, S_2, S_1)을 합성맵의 입력 변수 값 표 2의 (I_5, I_4, I_3, I_2, I_1)으로 사용하여 다음 표 3과 같이 작성하였다.

표 3에 보인 "$S(x)$의 입력변수"와 $S(x)$의 출력변수이며 동시에 "$L(S(x))$의 입력변수"로 연결되는 디지털회로에 관한 부울함수들은 식(1)로 구해졌고, "$L(S(x))$의 입력변수"와 "$L(S(x))$의 출력변수"에 관한 부울 함수들은 식 (3)으로 얻어졌으므로, 식 (1)과 식 (3)에 의해서 "삐뚤어진 혼돈합성 맵 $skewed\quad L_4(S_2(x))$"을 실현하는 디지털회로는 그림 3과 같이 설계 된다 [7],[8].

그리고 그림 3의 디지털 조합회로에 의해 수행되는 혼돈역학(chaotic dynamics)은 다음의 그림 4(0.0<x≤0.5), 그림 5(0.5<x≤1.0)와 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 선형궤환폐회로에 의해 반복 순환시킬 시에는, 길이가 각각인 순환주기들(cycles) - 10, 9, 6, 3, 2, 1 들을 갖는, 6개의 짧은 순환주기-에 의해서 총 31개의 혼돈상태(순서)들을 발생시킨다.

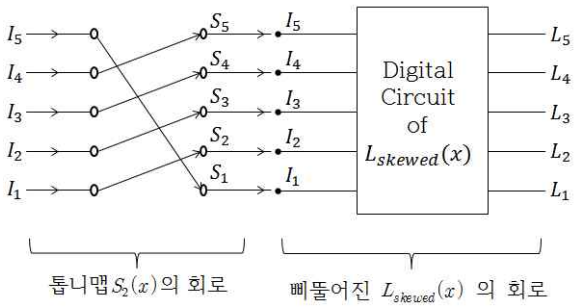

그림 3. 삐뚤어진 혼돈합성$skewed\quad L_4(S_2(x))$ 의 디지털 회로와 블록.

Fig. 3. Digital circuit and block of skewed logistic map$skewed\quad L_4(S_2(x))$.

표 3. 혼돈 합성맵 $L(S(x))$의 이산화 진리표.

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

변수 / 순서	$S(x)$의 입력변수					$L(S(x))$의 입력변수					$L(S(x))$의 출력변수				
	I_5	I_4	I_3	I_2	I_1	S_5	S_4	S_3	S_2	S_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	0	0	0	0	1	0	0	0	0	1
17	1	0	0	0	1	0	0	0	1	1	0	0	1	0	1
18	1	0	0	1	0	0	0	1	0	1	0	1	0	0	1
19	1	0	0	1	1	0	0	1	1	1	0	1	1	0	1
20	1	0	1	0	0	0	1	0	0	1	1	0	0	0	1
21	1	0	1	0	1	0	1	0	1	1	1	0	1	0	1
22	1	0	1	1	0	0	1	1	0	1	1	1	0	0	1
23	1	0	1	1	1	0	1	1	1	1	1	1	1	0	1
24	1	1	0	0	0	1	0	0	0	1	1	1	1	1	0
25	1	1	0	0	1	1	0	0	1	1	1	1	0	1	0
26	1	1	0	1	0	1	0	1	0	1	1	0	1	1	0
27	1	1	0	1	1	1	0	1	1	1	1	0	0	1	0
28	1	1	1	0	0	1	1	0	0	1	0	1	1	1	0
29	1	1	1	0	1	1	1	0	1	1	0	1	0	1	0
30	1	1	1	1	0	1	1	1	0	1	0	0	1	1	0
31	1	1	1	1	1	1	1	1	1	1	0	0	0	1	0

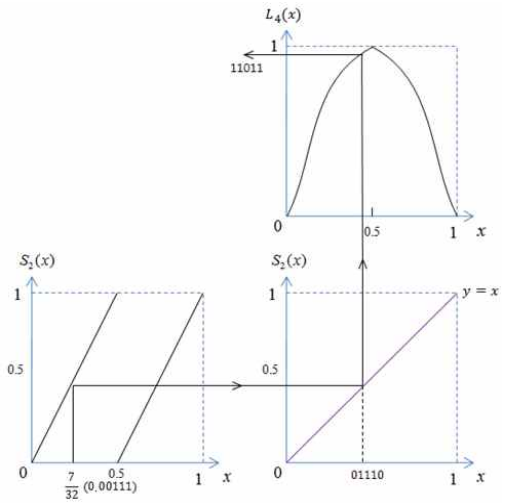

그림 4. 혼돈맵 회로에서 수행되는 이산2진값(00111)의 변환 예(0.0<x≤0.5인 경우)

Fig. 4. Conversion example on the chaotic composition map using discretized binary value(00111), (case of 0.0<x≤0.5)

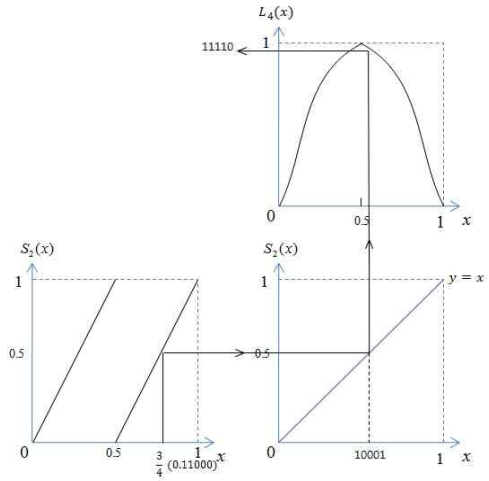

그림 5. 혼돈맵 회로에서 수행되는 이산2진값(11000)의 변환 예(0.5<x≤1.0인 경우)

Fig. 5. Conversion example on the chaotic composition map using discretized binary value(11000), (case of 0.5<x≤1.0)

예로 그림 4에 주어진 이산2진값(00111)에 의한 순환주기는 길이 9이며 다음과 같다.

00111
→01110→1(11011)→10111→2(10010)
→00101→3(01001)→10010→4(11100)
→11001→5(01110)→11100→6(01000)
→10000→7(11111)→11111→8(00010)
→00100→9(00111)

또한 그림 5에 주어진 이산2진값(11000)에 의한 순환주기는 길이 6이며 다음과 같다.

11000
→10001→ 1(11110)→11101→2(00110)
→01100→ 3(10111)→01111→4(11101)
→11011→ 5(01010)→10100→6(11000)

V. 결 론

이 논문에서 제시한 톱니함수와 삐뚤어진 로지스틱함수를 합성시킨 혼돈 합성맵에 관한 디지털조합회로의 경우, 5비트의 정밀도를 갖는 이산화 진리표 입력 변수부의 이산 2진값들을 입력으로 사용하면, 그림 4와 그림 5에서 보인 것처럼 혼동거동(chaotic behavior)를 내포하는 총 6개의 짧은 순환 주기를 발생시킬 수 있다.

그러므로 하나의 2진 키 값(binary key value)에 의해서 순환주기 31를 갖는 혼돈 2진 순서(혹은 수열)를 발생시키기 위해서는 궤환폐회로를 설계해야 하는 문제점을 갖는다.

이와 같은 문제점을 해결하는 방안으로는, 일련의 2^n-1개의 혼돈 2진 순서들을 모두 발생시킬 수 있도록 하기 위해서, 혼돈 합성맵 회로의 출력측과 입력측을 바로 연결하는 궤환폐회로(closed feedback circuit)보다는, 혼돈 맵회로의 입력측에 일련의 이산 2진 값들(random binary value)을 매클럭(1 clock)마다 입력시킬 수 있는 선형궤환시프트레지스터회로(linear-feedback shift register citcuit)를 연결시키고, 이 회로의 출력을 혼돈합성 맵회로의 입력으로 사용하는 것이 보다 효율적이다는 것을 실험을 통해 도출하였다.

즉, 혼돈 맵 디지탈조합회로의 입력측에 난수성 선형궤환시프트레지스터(LFSR)회로를 위치시키고 혼돈합성맵 회로의 출력들을 연결시킴으로써, 총 $(2^n-1)\times(2^n-1)$개의 혼돈 2진 순서들(chaotic binary sequences)을 발생시킬 수 있다.

Reference

[1] Heinz Georg Schuster, "Deterministic chaos", *Weinhem Germany : VCH Verlagsgesellschaft.* pp24~89, 1989.

[2] Heinz-Otto Peitgen,Hartmut Jürgens and Di-etmar Sa upe, "Farctals for the classroom", *Springer- verlag(N CTM), unit4,* PP.1~20,1991

[3] R.A.Rueppel, “Analysis and Design of stream ciphe r”, *Springer-Verlag, Berlin, Germany,* 1986.

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

[5] Kwang-Hyeon Park, Seung-Jae Baek, "Design of Rand om Binary Sequence Generator using the Chaotic Map ", *Journal of the Korea Contents Association,* v.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,* v.44, pp.253~255, 2009.

[7] Yong-Won Seo, Jin-Soo Park, "Design of the composit ion state machine based on the chaotic maps", *Journal of the Korea Academia-Industrial cooperation Society,* v.10, no.12, PP.3688-3693, 2009.

[8] Kwang-Hyeon Park, "Design of the digitla circuit composition state machine based on the chaotic comp osition function", *Journal of Chungju National Unive rsity,* v.45, pp.293~296, 2010.

박 광 현 (Kwang-Hyeon Park)

1977년 : 한양대학교 통신공학과 (공학사)
1995년 : 청주대학교 전자통신과 (공학박사)
1979~1995년 : 한국원자력연구소 (KAERI) 재직
1996년 ~ 현재 : 한국교통대학교 정보통신공학과 교수
관심분야 : 비선형통신회로, 혼돈역학, 스트림암호

서 용 원 (Yong-Won Seo)

2002년 2월 : 청주대학교 전자공학과 (공학사)
2004년 2월 : 청주대학교 전자공학과 (공학석사)
2013년 8월 : 청주대학교 전자공학과 (공학박사)
2006년 현재 : (주)이씨엠 대표이사
관심분야 : 스트림암호, 부호이론, 정보이론, 디지털통신