Journal of the Korea Academia-Industrial cooperation Society
Vol. 13, No. 9 pp. 4159-4164, 2012

http://dx.doi.org/10.5762/KAIS.2012.13.9.4159

암호통신 응용을 위한 전압제어형 카오스 신호 발생회로

주계초[1], 신봉조[2], 송한정[3*]
[1]인제대학교 나노시스템 공학부
[2]충북대학교 산학협력단부설 유비쿼터스바이오정보기술연구센터
[3]인제대학교 나노공학부

Chaotic Circuit with Voltage Controllability for Secure Communication Applications

Jichao Zhou[1], Bongjo Shin[2] and Hanjung Song[3*]
[1]**Derpartment of Nano Systems Engineering Inje University**
[2]**Research Institute of Ubiquious Bio-Information Technology of Joint Technology Research Center Chungbuk National University**
[3]**Derpartment of Nano Engineering Inje University**

요 약 본 논문에서는 암호통신을 위한 전압 제어형 카오스 신호 발생회로를 설계하였다. 제안하는 회로는 3개의 MOS 소자로 이루어지는 비선형 함수 블록과 소스 팔로워를 버퍼로 하는 이산형 카오스 신호 발생회로로, 비겹침 2상 클럭으로 구동되며, 2개의 제어전압 단자를 가진다. 제안된 회로는 SPICE 모의실험을 통하여 시간특성, 주파수특성 및 분기도 등의 여러 가지 카오스 다이내믹스가 생성됨을 확인하였다.

Abstract This paper presents a chaotic circuit with voltage controllability for secure communication applications. The proposed circuit which has two control voltages consists of the nonlinear function block(NFB) with three MOS transistors, one source follower and non-overlapping two-phase clock generator for sample and hold. By SPICE simulation, chaotic dynamics such as time waveform, frequency analysis and bifurcations were analyzed. SPICE results showed that proposed circuit can make various chaotic signals by control voltage.

Key Words : Nonlinear, Chaos, CMOS circuit, Time waveform, Bifurcation, Frequency analysis

1. 서론

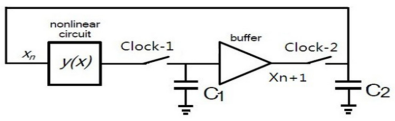
카오스 이론은 결정론적 운동방정식으로 설명되는 고전역학과는 달리, 자연계의 무질서한 현상으로부터 질서를 탐구하는, 근래에 주목받게 된 대표적인 비선형 동력학 이론의 하나이다 [1]. 이러한 비선형 동력계의 복잡한 카오스 현상을 전자회로로 구현해 보려는 시도는 그 동안 계속되어왔다 [2]. 1970년대에 발표된 추아회로가 대표적이며, 최근에는 반도체 집적회로로 이루어지는 여러 형태의 카오스 회로가 제안되었고, 이를 공학적으로 이용하려는 연구도 지속적으로 이루어지고 있다 [3]. 카오스 이론의 공학적, 특히 전자공학적 응용분야를 살펴보면 카오스 메모리, 다치논리 시스템, $\Sigma\Delta$ 변조기, 이미지프로세싱, 패턴인식, 카오스를 이용한 암호화 된 신호의 송수신, 카오스 뉴런을 이용한 인공지능 및 신경망 분야가 두드러지다 할 수 있다 [4]. 카오스 신호를 이용한 통신연구

본 논문은 IDEC(IC Design Education Center)의 지원 및 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(2012-0002777)
*Corresponding Author : Hanjung Song
Tel: +82-55-320-3873 email: hjsong@inje.ac.kr
접수일 12년 06월 08일 수정일 (1차 12년 07월 26일, 2차 12년 08월 31일) 게재확정일 12년 09월 06일

[5]는 카오스 신호의 초기치 민감성으로 인한 동기화 문제에 대하여, 1990년 Pecora[6]가 카오스 시스템을 적절한 부시스템으로 분리할 경우 조건적 동기화가 가능하다는 연구결과가 나오면서 활발히 연구되고 있다. 카오스 신호는, 연속형과 이산형으로 나뉠 수 있고, 연속형의 경우 로렌츠회로 또는 추아회로가 대표적이다 [2,3]. 이산형의 경우, 기본적으로 피드백을 지닌 차분방정식 형태로 표현이 되는데, 현재, 다양한 회로를 통하여 신호 구현이 연구되고 있다.모든 카오스 응용시스템에는 기본적으로 카오스 발생회로에 대한 하드웨어적인 전자회로 구현을 필요로 한다. 최근에 안정된 성능의 카오스 응용시스템 구현에는 카오스 신호 생성 회로의 제어용이성, 안정성, 저전력 및 소형화가 요구되어지게 마련이다 [7-10]. 본 논문에서는 암호화 통신을 위한, 전압제어가 가능한 이산형 카오스 신호 발생회로를 제안한다. 종래의 논문들[7-9]과는 다르게, 1개의 비선형함수와 1개의 소스팔로워(source follower)만으로 이루어지는 카오스 회로를 구현한다. 제안하는 카오스 집적회로는 이산시간 전압모드로 2상 클럭에 의해 동작되며, 카오스 신호 생성의 기본조건인 비선형성 구현에 필요한 비선형함수, 샘플앤드홀드 블록 등으로 구성된다. 제안하는 회로는 0.6 ㎛ 단일 폴리 2층 배선 CMOS 공정의 파라메타를 이용하여 SPICE 모의실험을 통하여, 시간파형, 주파수특성 및 분기도 등을 구하여, 카오스 현상을 분석한다.

2. 전압 제어형 카오스회로 설계

그림 1은 1개의 비선형 함수와 2상 클럭에 의해 구동되는 샘플앤드 홀드 블럭 및 버퍼로 구성되는 이산형 카오스 신호 생성회로의 예를 보여주고 있다.

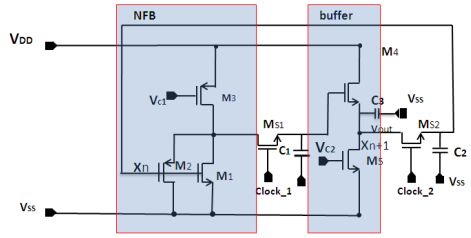


[그림 1] 일반적인 이산형 카오스 회로의 블럭도
[Fig. 1] General block diagram of the chaotic circuit for discrete chaotic signal

카오스 신호는 다음과 같은 차분 방정식을 통하여 표현될 수 있다 [8].

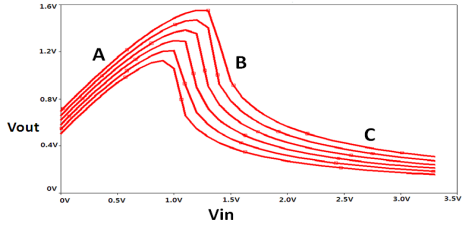
$$X(n+1) = f(X(n)) \qquad (1)$$

일반적으로, 카오스 신호생성에 필요한 비선형 함수를 어떻게 구현하느냐에 따라, 카오스 회로의 구조와 형태가 달라질 수 있다 [9].

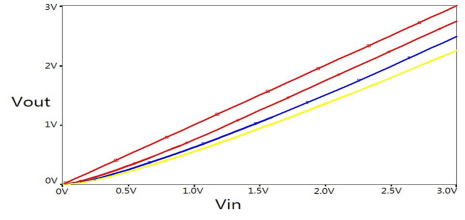


[그림 2] 제안하는 새로운 카오스 뉴런 회로
[Fig. 2] Chaotic circuit with voltage controllability

본 논문에서 구현하는 카오스회로를 그림 2에 나타냈다. 제안하는 회로는 비겹침 2상 클럭신호로 구동되며, 3개의 MOS로 이루어지는 비선형함수 NFB(nonlinear function block)와 소스 팔로워로 구성된다. 제안하는 회로는 동작 원리는, 카오스 생성회로의 입력 Xn 이 비선형함수회로(NFB)를 거치며 스위치 Ms1을 통하여, 소스 팔로워의 입력으로 연결되고, 그 출력 Xn+1이 스위치 Ms2를 거쳐 다시 입력으로 귀환된다. 비선형 함수 발생회로 NFB는 카오스 신호 생성에 필요한 비선형 함수를 구현한다. 그림 3은 NFB의 전달특성 곡선으로 영역 A는 양의 기울기, 영역 B는 음의 기울기를 가지며, 영역 C에서는 선형 특성을 가진다.

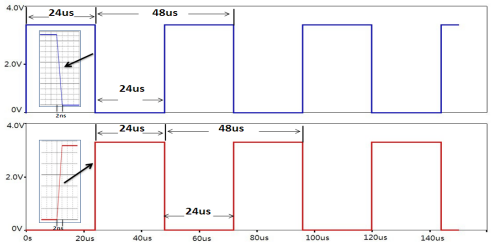


(a) 비선형함수 블럭의 전달특성 곡선



(b) 버퍼의 전달특성 곡선

[그림 3] 비선형함수와 버퍼 블럭의 전달특성곡선
[Fig. 3] Transfer curves of the nonlinear function block (NFB) and buffer block



[그림 4] 카오스 회로 구동 클럭 펄스
[Fig. 4] non overlapping clock pulse

그림 4는 본 논문에서 제안하는 이산형 카오스 회로 구동에 필요한 2상 비겹침(non overlapping) 회로의 클럭 펄스이다. 구동 클럭 주파수는 20 ㎑로 설정하였다.

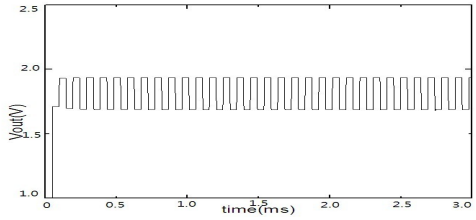
3. SPICE 시뮬레이션 결과

본 논문에서 제안하는 이산형 카오스 회로에 대하여 SPICE 모의 실험을 실시하였다. 사용된 SPICE 파라미터는 0.6 ㎛ CMOS 공정파라미터이다. 각종 MOS 트랜지스터와 커패시터 등에 대한 회로소자 값을 표 1에 나타내었다. 제안하는 회로는 전원전압 3.3 V, 클럭 주파수 20 ㎑에서 구동되도록 하였다.

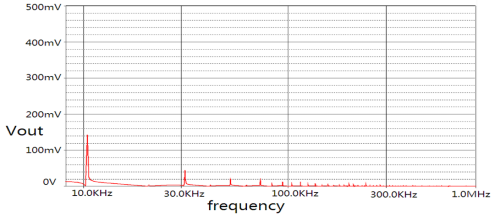
[표 1] 카오스 회로에 사용된 각종 소자 값
[Table 1] Device sizes for chaotic circuit

Device	Value	Unit
M1	W/L=1/0.6	㎛
M2	W/L= 4/0.6	㎛
M3	W/L=1/1	㎛
M4	W/L=15/0.6	㎛
M5	W/L= 1/5	㎛
M_{S1}, M_{S2}	W/L=2/0.6	㎛
C1, C2	5	pF
C3	20	pF
V_{DD}	3.3	V
Clock	20	㎑

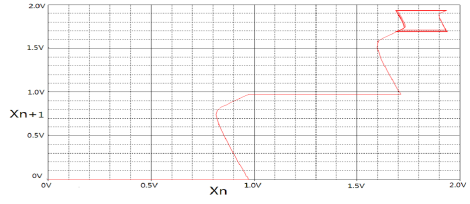
제어전압 Vc1의 변화에 따라 제안하는 회로의 카오스 특성 변화를 확인하였다. 그림 5는 제어전압 Vc2 = 1 V인 상황에서, Vc1 = 0.5 V 일 때의 출력 특성이다. 이 경우, 출력전압이 그림 5(a)에서 보듯이 2주기성의 특성을 보인다. 그림 5(b)는 출력전압의 주파수 특성으로 10.4 ㎑의 피크 주파수를 기준으로 31.3 ㎑, 52 ㎑에서 각각 제1, 제 2의 고조파 성분을 갖는다. 그림 5(c)는 카오스 회로의 출력에 대한 상태 천이도 (state transition diagram)으로 2주기성의 패턴을 그리고 있다. 그림 6은 제어전압 Vc2를 1 V로 고정한 상황에서, Vc1 = 1.23 V 일 때의 출력 특성이다. 이 경우, 출력전압이 그림 6(a)의 시간파형에서 보듯이 4주기성의 특성을 보인다. 그림 6(b)는 출력전압의 주파수 특성으로 5.2 ㎑, 10.4 ㎑, 15.6 ㎑, 20.8 ㎑에서 피크성분을 보인다. 그림 6(c)는 상태 천이도로 최종적인 궤적이 4주기성의 패턴을 그리고 있는 것을 보여주고 있다. 그림 7은 제어전압 Vc2를 1 V로 고정한 상황에서, Vc1 = 1.5 V 일 때의 출력 특성이다. 이 경우, 출력전압이 그림 7(a)의 시간파형에서 보듯이 카오스 특성을 보인다. 그림 7(b)는 출력전압의 주파수 특성으로 전체 주파수 영역에 걸쳐 주파수 성분이 분포하는 전형적인 카오스 신호 특성을 보이고 있다. 그림 7(c)는 카오스 회로의 출력에 대한 상태 천이도 로 최종적인 궤적이 카오스 패턴을 그리고 있는 것을 보여주고 있다.



(a) 시간파형

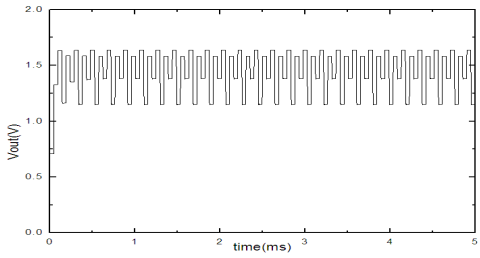


(b) 주파수 특성

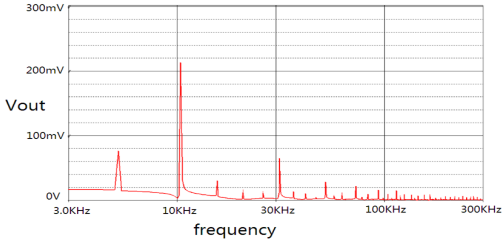


(c) 상태천이도

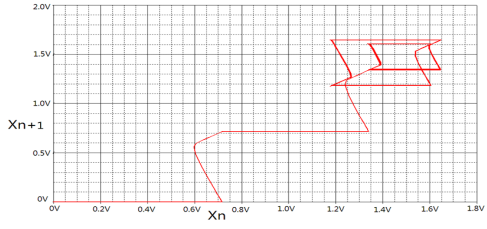
[그림 5] 2주기 출력특성.
[Fig. 5] Two periodic state (Vc1=0.5 V)



(a) 시간파형

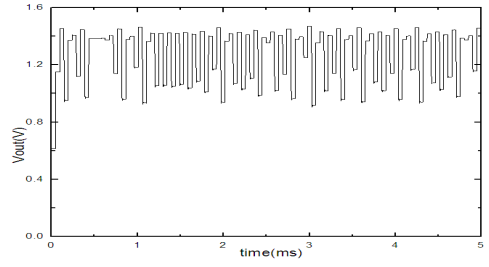


(b) 주파수 특성

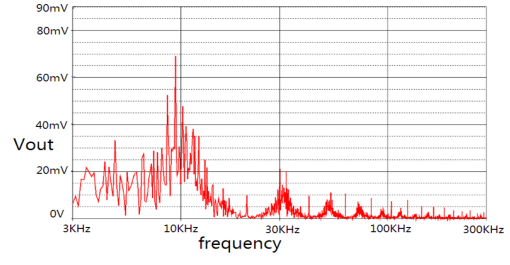


(c) 상태천이도

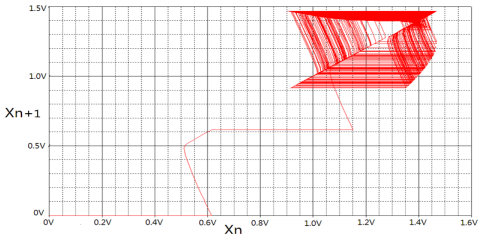
[그림 6] 4주기 출력특성.
[Fig. 6] Four periodic state (Vc1=1.23 V)



(a) 시간파형



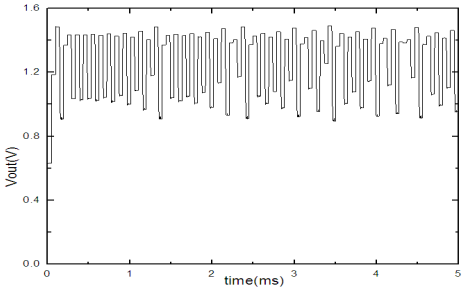
(b) 주파수 특성



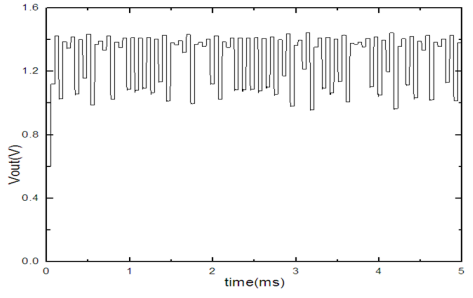
(c) 상태천이도

[그림 7] 카오스 출력특성.
[Fig. 7] Chaotic state (Vc1=1.5 V)

그림 8은 제어전압 Vc1를 1.5 V로 고정한 상황에서, 제어전압 Vc2를 변화 시켰을 때 각각 생성된 카오스 신호의 시간파형을 나타낸다. 그림 8(a)의 경우 Vc2 = 0.75 V 일 때의 카오스 특성, 그림 8(b)는 Vc2= 1.25 V일 때의 카오스 특성을 보인다.



(a) 생성된 카오스신호 (Vc2=0.75 V)

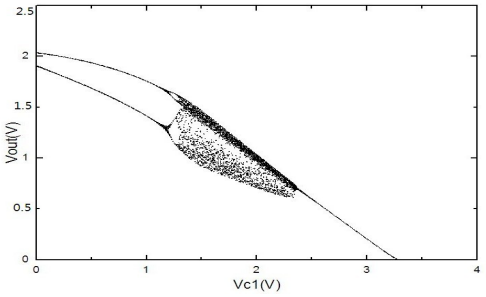


(b) 생성된 카오스신호 (Vc2=1.25V)

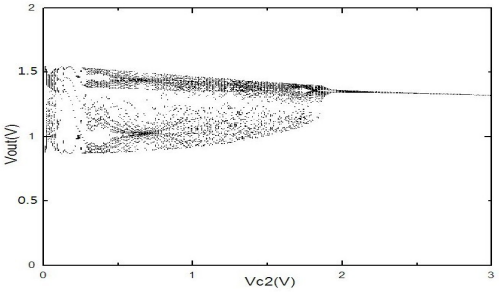
[그림 8] 다른 제어전압에 따라 생성된 따른 카오스 신호의 시간파형 (Vc1=1.5V 고정)
[Fig. 8] Time waveforms of chaotic signal according to different control voltage

마지막으로, 제어전압의 변화에 따른 분기도를 구하였다. 그림 9(a), (b)는 각각 제어전압 Vc1과 Vc2에 따른 분기도로, 그림에서 보듯이 제어전압 조건에 따라 주기상태에서 카오스 상태로 분기되는 것을 볼 수 있다. 결론적으

로, 특정한 제어전압 조건에서 카오스 신호가 생성됨을 보여주고 있다.



(a) Vc1에 따른 분기도 (Vc2=1V 고정)



(b) Vc2에 따른 분기도 (Vc1=1.5V 고정)

[그림 9] 제어전압에 따른 분기도
[Fig. 9] Bifurcations according to control voltage

4. 결론

본 논문에서는 전압제어가 가능한 카오스 신호 생성회로를 제안하였다. 제안하는 회로는 3개의 MOS 소자로 이루어지는 비선형 함수 블록과 소스팔로워 만으로 이루어지며, 2상 클럭으로 구동되며, 2개의 제어전압 단자를 가진다. 입력전압의 크기에 따라 주기 상태, 카오스 상태 등으로 분기됨을 시간파형과 입출력 전달특성을 통하여 확인하였다. 제안된 회로는 SPICE 모의실험을 통하여 시간특성, 주파수특성 및 분기도 등의 여러 가지 카오스 다이내믹스를 확인하였다.

Reference

[1] G. L. Baker, et al., Chaotic Dynamics an Introduction, Cambridge University Press, 1990.

[2] Kazuyuki Aihara, "Chaos engineering and its application to parallel distributed processing with chaotic neural networks," *Proceedings of the IEEE*, vol. 90, no. 5, pp. 919-930, May 2002.

[3] M. Delgado-Restituto, A. Rodriguez-Vazquez, "Integrated chaos generators," *Proceedings of the IEEE*, vol. 90, pp. 747-767, May 2002.

[4] K. Aihara, T. Takbe, and M. Toyoda, "Chaotic neural networks," Phys. Lett. A, vol.144, no.6, pp.333-340, 1990.

[5] Yongmei Cindy Wang, Applying Chaos in secure communications, Ph. D. thesis, Department of Electrical Engineering, Cornell University, May 1997.

[6] Louis M. Pecora and Thomas L. Carroll, "Synchronization of chaotic systems," Phys. Rev. Lett., vol. 64, Feb, 1990.

[7] H.J. Song and K.D. Kwack, ""CMOS circuit design and implementation of the discrete time chaotic chip"", ISCAS 2002, vol.III, pp.73-74, 2002

[8] P. Dudek and V.D. Juncu, "Compact discrete-time chaos generator circuit", Electronics Letters, Vol. 39, pp.1431-1432, 2003.

[9] D. Juncu, M. Rafiei-naeini and P. Dudek, "Integrated circuit implementation of a compact discrete-time chaos generator", *Analog Integrated Circuits and Signal Processing*, Vol. 46, no. 3, pp.275-280, March 2006.

[10] José L. Rosselló, et al., "A simple CMOS chaotic integrated circuit," *IEICE Electronics Express,* vol. 5, no. 24, pp. 1042-1048, December 2008.

주 계 초(Jichao Zhou) **[준회원]**

- 2008년 3월 ~ 2012년 2월 : 인제대학교 전자지능로봇공학과(공학사)
- 2012년 3월 ~ 현재 : 인제대학교 나노공학부 (석사과정)

<관심분야>
반도체, 회로설계, 소자

신 봉 조(Bongjo Shin) **[정회원]**

- 1991년 2월 : 숭실대학교 반도체공학과 (석사)
- 2000년 2월 : 충북대학교 전자공학과 (박사)
- 1987년 11월 ~ 2000년 5월 : 현대전자산업(주) 책임연구원
- 2000년 4월 ~ 2004년 6월 : 충북대학교 BK 부교수
- 2004년 9월 ~ 현재 : 충북대학교 유비쿼터스바이오정보기술연구센터 개발실장

<관심분야>
반도체, 정보통신

송 한 정(Han-Jung Song) **[정회원]**

- 1986년 2월 : 한양대학교 전자공학과 (공학사)
- 1988년 2월 : 한양대학교 전자공학과 (공학석사)
- 2000년 2월 : 한양대학교 전자공학과 (공학박사)
- 2004년 3월 ~ 현재 : 인제대학교 나노공학부 부교수

<관심분야>
반도체 소자 신뢰성 및 회로설계