https://doi.org/10.21289/KSIC.2021.24.5.635

0.18um CMOS 공정을 사용한 카오스 난수 발생기 분석

Analysis of Chaotic True Random Number Generator Using 0.18um CMOS Process

정예찬[1], 차민드라[1], 알라딘[1], 이송욱[1], 니 한[2], 송한정[3*]

Ye-Chan Jung[1], Chamindra Jayawickra[1], AlaaDdin Al-Shidaifat[1], Song-Wook Lee[1], Nihan Kahrama[2], Han-Jung Song[3*]

〈Abstract〉

As times goes by, a ton of electric devices have been developing. Nowadays, there are many personal electric goods that are connected each other and have important private information such as identification, account number, passwords, and so on. As many people own at least one electric device, security of the electric devices became significant. To prevent leakage of the information, study of Chaotic TRNG, “Chaotic True Random Number Generator”, protecting the information by generating random numbers that are not able to be expected, is essential. In this paper, A chaotic TRNG is introduced is simulated. The proposed Chaotic TRNG is simulated with Virtuoso &, a circuit design program of Cadence that is a software company. For simulating the mentioned Chaotic TRNG, setting values, 0V low and 3V high on Vpulse, 1.2V on V-ref, 3.3V on VDD, and 0V on VSS, are used.

Keywords : Chaos, Randomness, Security, TRNG

1 인제대학교 나노융합공학과
2 Yildiz Technical University, 이스탄불, 터키
3* 교신저자, 인제대학교 나노공학부, 나노매뉴팩처링 연구소, 정교수 E-mail: hjsong@inje.ac.kr

1 Dept. of Nanosciences and Engineering, Inje University
2 Department of Electronic and Communication Engineering, Yildiz Technical University, Istanbul, Turkey
3* Dept. of Nanosciences and Engineering, Inje University, Center for Nano Manufacturing, Inje University

1. 서 론

오래전부터 지금까지 많은 기술적 발전이 있어왔고 기술이 비약적으로 발전하는 특정 시기가 역사적으로 여러 번 있어왔다. 가장 최근에 일어난 기술적 발전의 산유 물은 스마트폰이라고 할 수 있다. 스마트폰이 출시 된 이후로 수많은 스마트폰, 태블릿, 애플워치, 경량화 된 소형 노트북 등과 같은 휴대하기에 용이하고 기기들 끼리 서로 호환되어 소통하는 IoT 기술이 발전하였다. 전자기기들이 서로 소통하는 만큼 유출되어서는 안 되는 소유자의 중요한 개인적인 정보들이 기기 들 사이에 공유가 되고 있으나 그에 따른 정보의 유출에 대해서는 아직까지 대중적으로 인식되어 있지 않지만 대기업들의 고객정보 유출과 개인이 개인정보의 유출로 인하여 피해를 보는 사례들이 많아짐에 따라서 전자기기의 보안에 더욱 더 많은 사람들이 관심을 가지고 보안을 제품을 선택하는 요소 중에 하나가 될 만큼 인식의 변화가 생기고 있다. 보안을 강화하기에는 여러 방법들이 있는데 그중에 난수를 생성하는 난수 발생기가 있다[1-4]. 기존의 난수 발생기에는 정해진 패턴이 있어 그 한계점을 가지고 있다. 하지만 카오스 신호를 이용하여 난수를 발생시키면 기존의 난수발생기와는 다르게 예상할 수 없는 난수를 발생시켜 보안을 강화할 수 있다[5-7]. 이 논문에서는 카오스 난수발생기를 Cadence사의 Virtuoso &를 이용하여 시뮬레이션하여 그 결과 값을 도출해보고 해석해 보았다.

2. 로렌츠 방정식

카오스신호를 발생시키기 위해서는 먼저 카오스에 대한 이해가 필요하다. 미국의 기상학자 에드워드 로렌츠는 나비효과 개념을 이야기하였는데 그의 나비효과 개념은 카오스 이론의 토대가 되었고 로렌츠 방정식을 만들었다[8-10]. 따라서 카오스 난수발생기를 이해하기 위해서는 로렌츠 방정식을 알아야 한다. 로렌츠 시스템 안에는 세 개의 다른 방정식이 있으며 이 세 개의 방정식은 간단하지만 카오스 한 결과를 보여준다. 앞서 언급한 로렌츠 방정식은 다음과 같이 각각의 x, y, z는 3차원 공간에서 아래와 같이 주어진다.

$$\dot{x}(t) = p(y(t) - x(t)) \quad [8]$$
$$\dot{y}(t) = rx(t) - y(t) - x(t)z(t) \quad [8]$$
$$\dot{z}(t) = x(t)y(t) - bz(t) \quad [8]$$

위의 세 가지 로렌츠 방정식에서 변수 x, y, y는 시간에 따라 변경 될 수 있다. 카오스 한 결과 값을 얻기 위해서는 변수 p, r, b에 특정한 상수 값이 있어야하며 그 값들은 변수 p에는 10, 변수 r에는 35.5 그리고 변수 b에는 8/3이 할당되어야 한다.

로렌츠 방정식을 실질적으로 실현하려면 오일러의 공식을 사용하여 방정식을 이산 형식으로 써야한다.

$$X(K+1) = X(K) + ts(p(Y(k) - X(k))) \quad [8]$$
$$Y(k+1) = Y(k) + ts(X(k)(r - Z(k)) - Y(k)) \quad [8]$$
$$Z(k+1) = Z(k) + ts(X(k)Y(k) - bZ(k)) \quad [8]$$

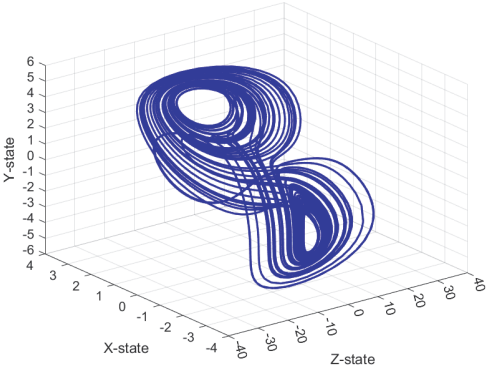

Fig. 1 A three-dimensional graph shown using the attractors X, Y, and Z in the Lorentz equation

3. 카오스 난수발생기 시뮬레이션

이 논문에서는 Cadence사의 Virtuoso & 프로그램을 이용하여 카오스를 이용한 난수발생기 TRNG(True Random Number Generator)회로를 특정한 조건에서 시뮬레이션 하였다. 제안된 카오스 난수발생기의 결과 값을 도출하기 위해서 V_pulse에 low 0V, high 3V, period 1u second, delay 1p second, rise 1p second, fall 1p second, width 500n second를 V_ref에는 1.2V를 VDD에는 3.3V를 인가하였다. 시뮬레이션의 결과 값을 C1_connect, Q-out, Q2-out과 Q1에서 Q16핀을 사용하여 결과 값을 도출하였다. 다음은 그 제안된 카오스 난수발생기의 회로와 시뮬레이션의 결과 값들이다.

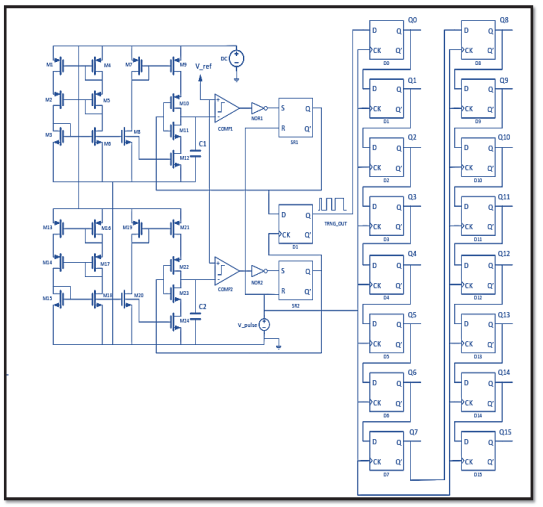

Fig. 2 Schematic of the proposed chaos random number generator

위의 그림에서 왼쪽의 카오스 회로를 통해 나온 카오스 신호가 오른쪽의 Q1부터 Q16까지의 D-Latch에 들어가 난수를 발생 시키는 구조임을 확인할 수 있다.

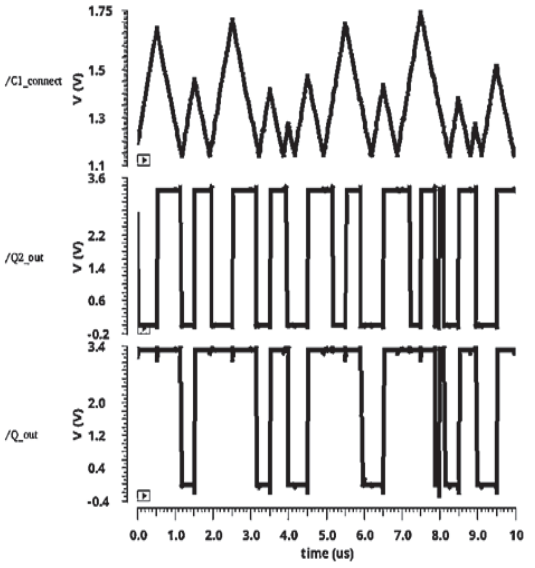

Fig. 3 Output values obtained through C1_connect, C2_out, Q_out pins

위의 출력 그래프를 보면 카오스 신호를 생성하기위해서는 커패시터가 필요한데 가장위에 있는 C1_connect에서 커패시터가 충전 방전을 하는 것을 알 수가 있다. 두 번째 Q_out은 출력된 일정한 패턴을 가지지 않는 카오스 신호이다. 마지막 Q2_out 또한 Q_out과 같이 카오스 신호이다.

여기서 Q_out과 Q2_out을 측정한 이유는 서로 다른 두 개의 카오스 신호를 합하여 좀 더 난해한 카오스 신호를 D-Latch에 전달하기 전에 각자의 출력 값들이 패턴을 가진 신호가 아니라 카오스 신호임을 보여주기 위함이다.

아래의 그래프를 보면 각자의 출력단자가 각자 다른 패턴을 가진 것을 볼 수가 있다. 1초 단위로 볼 때 전압이 0V일 때는 숫자0을 전압이 1V일 때는 숫자1을 나타낸다. 따라서 시간이 지나감에 따라 처음에는 출력되는 숫자가 일정패턴을 가지는듯하게 보이나 패턴이 일정하지 않게 변화하며 예측할 수 없는 난수가 발생함을 알 수가 있다.

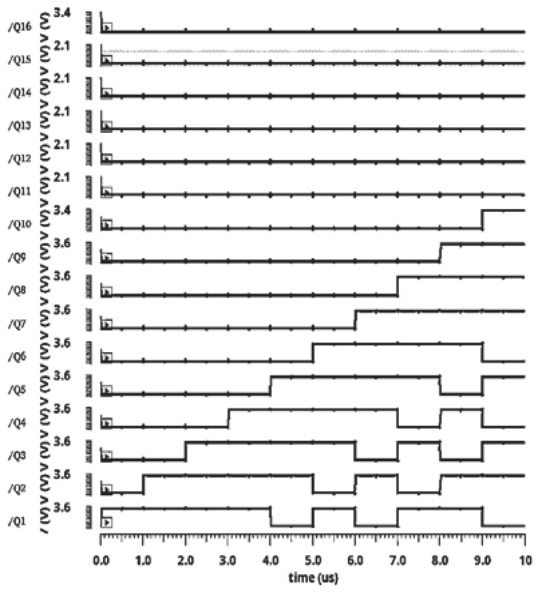

Fig. 4 Output graph from Q1 to Q16 output through chaos signal

4. 결 론

이 논문을 통하여 로렌츠 방정식이 어떻게 일정하지 않은 패턴을 가진 카오스 형태를 뛰는지 X,Y,Z 어트랙터를 통해 그래프로 알 아 보았다. 카오스 난수 발생기가 어떻게 구성되어 있는지 회로도를 통해 알 아 보았다. 카오스 난수 발생기의 시뮬레이션을 통하여 카오스 난수 발생기의 작동 방식과 그 안에 있는 각각의 블록들의 역할과 각각의 회로가 카오스 신호를 발생 시 키는데 왜 필요한지 알 아 보았다. 시뮬레이션의 분석을 통하여서 카오스 회로 이론이 회로 상에서 구현이 가능함을 알 아 보고 실질적으로 구현 가능함을 알 아 보았다. 결과적으로 시뮬레이션의 결과가 이상적으로 이루어 졌으나 시뮬레이션의 출력 값을 보면 더욱더 난해하고 전혀 연관성이 없어 보이는 출력 값을 가지는 카오스 신호를 통해서 카오스 난수 발생기가 더욱더 발전할 여지가 있음을 알 수가 있었다. 갈수록 커져가는 보안의 중요성만큼 카오스와 난수발생기의 연구가 연구로써의 가치가 뛰어남을 알 수 있었다. 카오스회로와 난수발생기가 더욱 더 많은 관심을 받고 연구가 이루어진다면 이 분야가 더욱 더 발전할 것으로 기대된다.

Acknowledgement

This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (NRF-2019R1F1A1056937). The chip fabrication and EDA tool were supported by the IC Design Education Center(IDEC), Korea.

참고문헌

[1] Petrie, Craig S., and J. Alvin Connelly. “A noise-based IC random number generator for applications in cryptography.” IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications 47.5 (2000): 615-621.

[2] Bucci, Marco, et al. “A high-speed oscillator-based truly random number source for cryptographic applications on a smart card IC.” IEEE transactions on computers 52.4 (2003): 403-409.

[3] Bagini, Vittorio, and Marco Bucci. “A design of reliable true random number generator for cryptographic applications.” International Workshop on Cryptographic Hardware and Embedded Systems. Springer, Berlin, Heidelberg, 1999.

[4] Callegari, Sergio, Riccardo Rovatti, and Gianluca Setti. “Embeddable ADC-based true random number

generator for cryptographic applications exploiting nonlinear signal processing and chaos." IEEE transactions on signal processing 53.2 (2005): 793-805.

[5] Pivka, Ladislav, Chai Wah Wu, and Anshan Huang. "Chua's oscillator: A compendium of chaotic phenomena." Journal of the Franklin Institute 331.6 (1994): 705-741.

[6] Rössler, Otto E. "An equation for continuous chaos." Physics Letters A 57.5 (1976): 397-398.

[7] Dedieu, Herve, Michael Peter Kennedy, and Martin Hasler. "Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits." IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing 40.10 (1993): 634-642.

[8] Lorenz, Edward N. "Deterministic nonperiodic flow." Journal of atmospheric sciences 20.2 (1963): 130-141.

[9] Yang, Qigui, and Caibin Zeng. "Chaos in fractional conjugate Lorenz system and its scaling attractors." Communications in Nonlinear Science and Numerical Simulation 15.12 (2010): 4041-4051.

[10] Cuomo, Kevin M., Alan V. Oppenheim, and Steven H. Strogatz. "Synchronization of Lorenz-based chaotic circuits with applications to communications." IEEE Transactions on circuits and systems II: Analog and digital signal processing 40.10 (1993): 626-633.

(접수: 2021.09.17. 수정: 2021.10.04. 게재확정: 2021.10.06.)