한국산학기술학회논문지
Vol. 5, No. 4, pp. 321-325, 2004

# 출력난수열의 랜덤성을 고려한 H/W 발생기에 관한 연구

홍 진 근*

# A study on H/W generator with randomness of output random stream

**Jin Keun Hong***

**요 약** 하드웨어 부품으로 구성된 실난수 발생기는 그 특성상 편이성을 갖지 않는 안정된 출력 난수열을 지속적으로 제공하는 것이 어렵다. 본 논문에서는 실난수 발생기에서 추출된 출력 난수열의 편이성을 갖는 통계적 특성을 감소하는 방안에 관해 연구하였다. 제시한 방안은 FIPS 140-1에서 제시하고 있는 랜덤성(randomness)의 조건을 만족하도록 출력 난수열의 랜덤성(randomness)을 개선하였다.

**Abstract** It is quite difficult to create an unbiased and stable random bit stream, as required for statistical randomness, when using a random generator with only a hardware component. In this paper, we studied to reduce the statistical property of the biased bit stream in the output of a real random number generator. The proposed scheme is enhanced the randomness of output bitstream, these test items are used by FIPS 140-1.

**Key Words :** random number generator, randomness, biased bit sequence

## 1. 서 론

암호학 프로토콜에서는 강인한 암호학 일수록 안전한 난수열을 요구하고, 공격자에게 알려지지 않아야 하는 비밀 값이 생성되고 사용되어야 한다. 일반적으로 암호학에서 사용되는 암호방식에는 대칭형태의 암호방식과 비대칭형태의 암호방식으로 분류한다. 비대칭형 암호방식은 RSA(Rivest, Shamir, Adleman), D-H (Diffie, Hellman) 등이 제안한 공개키 개념을 바탕으로 개인키/공개키를 디지털서명 등과 같은 곳에 적용하고 있으며, 대칭형이나 하이브리드 암호시스템에서 사용되는 난수는 데이터 암호목적으로 주로 사용되고 있다. 난수열을 생성하는 실난수 발생기는 통계적인 랜덤성(randomness)을 제공하기 위해 자연 현상으로부터 추출 가능한 비예측적이고 모조할 수 없는 비결정적인 잡음원을 사용한다. 의사난수발생기의 경우 초기화 시드(seed) 값을 제공 받기 위해 실난수 발생기를 사용하지 않고는 안전성을 보장 받을 수 없다. 발생기의 시드(seed) 값은 완전한 랜덤성(randomness)을 제공하는 소스를 요구하지만 결정적인 시스템에서는 완전한 랜덤성(randomness)을 제공하는 소스를 생성시키는 것이 불가능하다. 비결정적인 출력난수를 제공하는 실난수 발생기의 경우 마찬가지로 보편적인 하드웨어를 사용하는데, 그 특성상 속도가 느리고, 구현이 어려우므로 성능이 보장되지 않는 하드웨어라는 전제를 필요로 한다.

실난수 발생기를 설계할 때, 기존 연구에서는 하드웨어로 구현된 실난수 발생기가 적합한 통계적 랜덤성(randomness)을 제공하기 위해, 실난수 발생기에 해쉬함수(hash function)를 결합하거나를 이용함으로써 실난수 발생기가 갖는 한계성을 해LFSR (linear feedback shift register)이 결합된 모델로 해결하려는 연구가 있었다[1-4]. 그러나 해쉬함수나 의사난수발생기(LFSR)이 결합된 모델의 경우 출력 난수열의 통계적인 랜덤성(randomness)이 해쉬함수나 의사난수발생기의 특성에 결정되어진다. 또한 설계 및 시드(seed) 값 관리와 같은 어려움이 있다. 1951년 존 폰 노이만[5]은 "0"와 "1" 비트의 균일한 분포를 제공하기 위한 방식으로 비트 교정 개념을 제안하였고, 이를 근거하여 비트 교정기라는 하드웨어에 의해 초기 난수성 측정이 이루어졌다. 노이만 교정기는 출력 난수 비트쌍을 하나의 비트로 맵핑(mapping)하여 변환함으로써 편이성을 갖는 출력 난수열에 대해 통계적으로 편이성을 갖지 않는 출력 난수열을 생성시키는 간단한 방식으로 이용되고 있다. 그러나 이 방식은 출력 난수열의 비트 중복성을 제거함으로써

*천안대학교 정보통신학부
E-mail: jkhong@cheonan.ac.kr
Tel: 041-620-9445

실난수 발생기의 전체 출력 난수열의 랜덤성(randomness)에 영향을 준다. 본 논문에서는 편이성을 갖는 출력 난수열에 대해 주어진 듀티 사이클(duty cycle) 동안 출력 난수 "0"나 "1" 비트의 분포를 파악하고, 출력 비트의 듀티 정보를 이용하여 출력 난수열을 안정화시킴으로써 편이성을 갖지 않도록 출력 난수열을 얻도록 하였다. 출력 난수열을 안정화 시키는 방안으로서 주어진 기간동안 전체 출력 난수열 가운데 "1"비트의 밀도분포를 파악하고 분포가 0.5의 값을 갖도록 유도하였다. 이때 안정화된 출력 난수열은 편이성을 갖는 출력 난수열에 비해 FIPS 140-1[6]에서 제시하는 난수 발생기의 랜덤성(randomness) 검증조건을 만족하는 것을 확인하였다. 본 논문의 구성은 다음과 같다. 2장에서는 실난수 발생기 출력수열의 특성을 언급하고, 3장에서 제안된 반전처리 알고리즘에 대한 원리를 기술한다. 4장에서는 시뮬레이션 환경 및 결과에 대해 살펴보고, 5장에서 결론을 맺는다.

## 2. 실난수 발생기의 출력수열의 특성

적용된 잡음원은 백색 가우스 잡음으로서 주어진 대역폭에 비례하는 잡음전력을 갖는다. 가우스 잡음은 가우스 진폭분포를 갖는다. 가우스 잡음 분포함수 의 확률밀도는 식(1)에서와 같이 정의할 수 있다.

$$f(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{x^2}{2\sigma^2}} \quad (1)$$

여기서 σ는 가우스 잡음전압의 실효 값이고 실난수 발생기의 잡음 전력밀도는 진폭이 가우스 분포를 갖는다.

추출되는 잡음은 비교기에 의해 편이성을 갖지 않는 출력 난수열을 얻기 위해 일정하게 증폭되며, 잡음원의 비교기를 통한 "1", "0"비트 패턴 식별 및 샘플링 과정을 거친다. 잡음원 추출은 미약한 잡음 AC신호를 검출하고, 이를 추출 가능한 크기로 사용하기 위해 연산 증폭과정을 거친다. 잡음 출력파형은 주파수의 백색잡음 분포를 가지고, 순시진폭은 가우스 분포를 따른다. 적용된 잡음 신호는 DC성분을 제거하기 위해 고역통과필터(HPF)를 이용한 필터 출력단에서 얻어진 AC 소신호를 사용한다. 패턴 식별을 위한 비교기는 영교차 레벨을 기준으로 패턴을 식별한다. 비교기 출력단은 입력 AC 소신호의 레벨 변동이 비교기의 교차점을 기준으로 "1", "0"비트 레벨은 천이가 일어나고, 이때 얻어진 비교기의 출력은 샘플링 과정의 입력 값으로 결정한다. 그런데 실난수 발생기는 전자회로 설계된 디바이스, 온도, 주변 환경 등에 민감한 영향을 받게 되므로 잡음 출력 난수열이 편이성을 가지게 된다.

## 3. 제안된 알고리즘 원리

반전처리 알고리즘은 편이성을 가진 출력 난수열로부터 통계적으로 균일한 분포를 갖도록 처리하는 방안이다. 실난수 발생기에서 편이성을 갖지 않는 출력 난수열이 생성되기 위해서는 "0"와 "1"의 비트 밀도분포가 균일하게 나타나야 한다. 제안된 반전처리 알고리즘은 듀티 정보를 이용한다. 듀티는 한 사이클을 20000비트로 하고 편이성을 개선시키기 위한 중요 척도로 사용되며 식(2)와 같이 나타낸다.

한 주기동안 밀도분포를 균일하게 처리하기 위해 고려될 수 있는 반전처리는 주어진 사이클 동안 홀수비트의 반전("0" "1", "1" "0")을 수행하는 방안과 4비트를 단위로 하여 1번째 비트만을 반전 처리하는 방안을 고려할 수 있다. 출력 난수열이 아래와 같이 연속적인 분포로 나타날 때, "1"비트의 듀티는 전체T가 40이고, "1" 비트의 수 t 는 12이다. 따라서 듀티(t/T)는 12/40이므로 0.3이다.

방안1에 의한 반전 처리를 적용하면 아래의 패턴을 얻을 수 있고 이때 듀티는 20/40으로0.5가 된다.

위의 경우 "0"와 "1"의 밀도분포 측면에서 살펴보면 균일한 분포를 갖게 된다. 그런데 4비트의 패턴이 전체 16개의 패턴 가운데 특정패턴 값만 나타나게 되므로 포커검증 측면의 경우 불균일하게 분포하므로 전체적인 편이성을 개선하는데 한계가 있다. 방안2에 의한 반전처리를 이용한 개선하는 방안으로 4비트 가운데 특정비트만 반전처리를 수행하는 것으로 처리결과는 아래의 패턴과 같다.

이 경우 듀티는 16/40으로 0.4 값으로 전체를 반전처리하는 방안보다 1/2 주기로 나누어 반전처리를 수행하는 방안이다. 그러나 이러한 방안도 근본적으로 개선할 수 있는 적합한 방안이 아니다. 따라서 본 논문에서는 일정 주기동안(20000비트 단위) 듀티를 0.5로 고정시키고 출력 난수열의 값이 0.5를 중심으로 하는 유의수준 결정 값과 실제 나타나는 "1"비트 수의 옵셋 차이만큼 반전처리를 수행하고, 반전 처리되는 위치에 대한

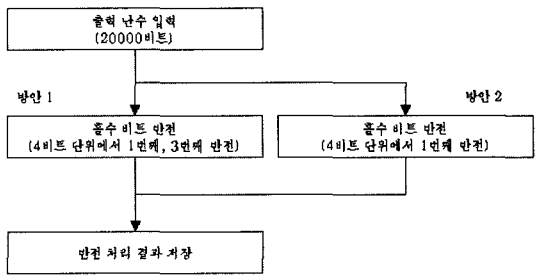


Fig. 1. 반전처리 방안 1과 방안 2 처리흐름

결정은 카오스 함수를 사용한다.

$$D = \frac{t(\text{“1” 비트 수})}{T(2000\text{비트})} \quad (2)$$

여기서 D 값은 “1”비트 수를 T로 나눈 값으로 정의된다.

제안된 알고리즘 처리과정은 그림 2에서 제시하였는데 먼저 출력 난수열 20000비트가 입력되고, 듀티를 계산하기 위해 “1” 비트 수를 계산하여 저장한 후 듀티를 계산한다. 계산된 듀티 값이 정의된 유의수준 범위 이내에 있으면 편이성이 없다고 판정하고 해당 난수열은 반전처리를 수행하지 않고 저장된다. 그러나 유의수준 범위 밖에 값을 가지면 즉 반전처리를 수행한다. 이때 정의된 유의수준 범위는 20000비트에 대해 FIPS 140-1에서 명시하고 있는 모노비트 검증항목을 근거하여 결정된 값으로 “1” 비트 수가 9654~10346 값 사이의 범위로 결정하였다. 한 사이클동안 출력 난수열 “1”비트 수가 유의수준 범위 밖일 때 반전처리를 수행하게 되는데, “1” 비트 수가 9654개 이하이면 (9654- “1” 비트 수) 차이 값 만큼 “0” 비트를 “1”비트로 반전처리를 수행한다. 이와 반대로 “1” 비트 수가 10346개 이상이면 (“1” 비트 수 10346) 차이 값 만큼 “1” 비트를 “0” 비트로 반전처리를 수행한다. 이때 반전처리는 카오스 함수의 랜덤한 출력 값을 근거하여 비트 반전을 수행하고, 20000비트내에서 동일한 위치에서 반전은 1회로 제한된다.

이산 카오스 시스템[7-9]은 그 특성상 불결정적이고 비예측성을 갖는 시스템(nonlinear deterministic system)으로 그 신호는 비주기적인 불규칙성을 가지면서 상태

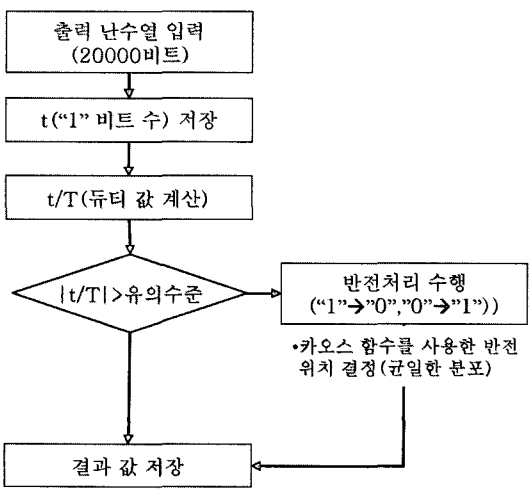


Fig. 2. 제안된 반전처리 방안 흐름도

공간의 어떤 영역 내부로 제한되어 있다. 또한 카오스 신호는 극히 근접한 초기 조건을 가지는 시스템으로부터 발생하더라도 일정 시간이 경과하면 전혀 다른 궤적을 나타내므로 초기조건에 매우 민감한 특성을 가진다. 그리고 카오스 함수는 초기 값, 파라미터 등의 모든 조건이 완전히 일치하지 않으면 전혀 다른 난수를 발생시킨다. 이러한 카오스 신호의 특성은 정보의 은닉을 위한 암호통신에 적합하게 이용되고 있다[10-13].

본 논문에서는 주어진 사이클 동안 반전 위치를 결정하기 위해 요구되는 난수를 이산 카오스 함수를 적용하였다. 적용된 이산 카오스 사상인 로지스틱 함수는 식 (3)에서 제시한 바와 같다[14].

$$X_{n+1} = -\alpha X_n(1 - X_n) \quad (3)$$

이때 파라미터 $\alpha$는 $0 \le \alpha \le 4$ 의 범위를 가지고, 초기값 $X_n$의 범위가 $0 \le X_0 \le 1$ 일 때 $X_{n+1}$은 바로 이전 상태 값인 $X_n$으로부터 결정된다. 그러나 이에 역으로 $X_{n+1}$이 주어질 때 가능한 $X_n$은 2차 방정식의 해가 되므로 2개의 값을 가진다. 로지스틱 사상은 비가역적인 특성을 갖는다. 이때 $\alpha$는 초기 값에 대한 다음 값의 의존성을 나타내는 감도 파라미터(sensitivity parameter)로서 $\alpha$가 클수록 초기 값의 미소한 변화가 반복된 계산에 의해 현저한 차이를 갖는다. 카오스 함수의 출력은 한 사이클(1~20000비트) 동안 반전위치를 균일한 분포로 발생시키고, 발생된 위치정보를 이용하여 해당 비트반전(“0”→“1”, “1”→“0”)을 수행한다.

## 4. 실험 환경 및 결과

실난수 발생기의 출력 난수열이 편이성 여부를 진단하기 위해 사용된 척도는 FIPS 140-1 난수발생기의 난수성 검증 항목인 모노비트 검증, 포커검증, 런 검증이다[6]. 실난수 발생기로부터 얻어진 랜덤 비트열은 제시된 각 테스트 항목에 대해 검증이 수행되었고, 이에 대한 결과를 그림 3에서 그림 5에 나타내었다. 검증을 위해 실난수 비트열은 20000비트를 10개에 대한 통계적 검증을 실시하였다. 모노비트검증은 출력수열의 랜덤성(randomness)을 측정하는데 가장 중요한 기본요소가 되며, 편이성이 이상적으로는 “1”비트의 분포와 “0”비트의 분포가 50 : 50의 분포를 가지게 된다. 편이성이 심한 출력 난수열에 대한 모노비트 검증을 수행하면 “1” 비트 수가 10000비트(듀티가 0.5)보다 변동폭이 심한 값(큰 값 또는 작은 값)을 갖고 반전처리 방안 1 보다 방안 2의 결과가 개선된 것으로 나타난다. 그러나 방안 2의 경우도 출력 난수열의 편이 성질이 특정 비트 패턴

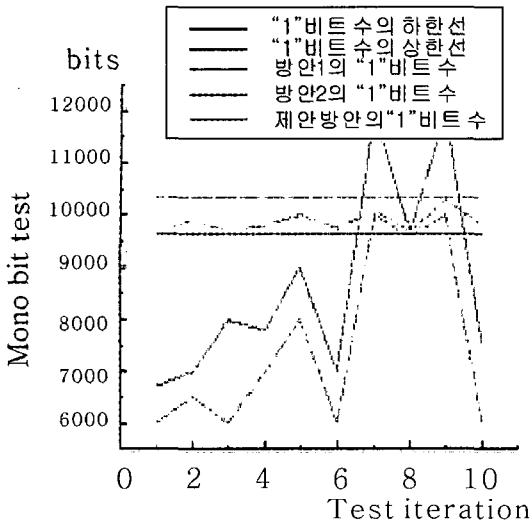


Fig. 3. 모노비트 검증항목에서 반전처리 방안1, 2와 제안방안의 결과 비교

에 종속적인 것으로 나타난다. 제안된 방안은 주어진 출력 난수열이 편이성을 갖는다 하더라도 차분 성분만큼 비트반전을 보상해줌으로써 모노비트 검증항목을 통과하는 것으로 나타났다. 포커 검증항목은 4비트 클래스가 주어진 사이클에서 16개 패턴을 갖게 되고, 16개의 패턴이 얼마의 빈도를 가지고 나타나는가를 검증하게 된다.

마찬가지로 반전 처리 방안 1과 방안 2의경우 반전처리 알고리즘이 출력 난수열의 패턴에 종속되기 때문에 포커검증의 유의수준을 만족시킬 수 없다. 그러나

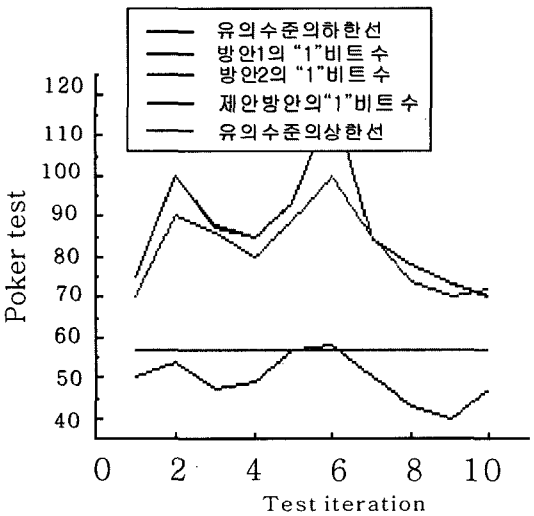


Fig. 4. 포커 검증항목에서 반전처리 방안 1, 2와 제안방안의 결과 비교

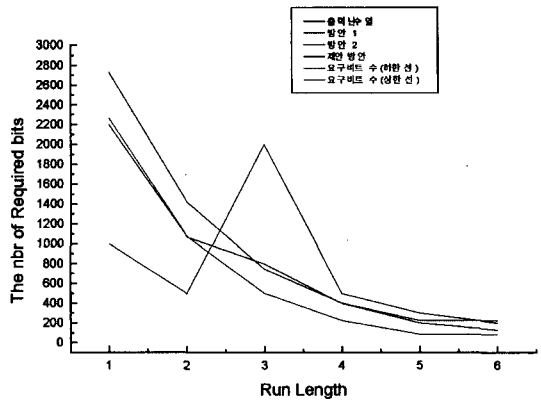


Fig. 5. 런 검증항목에서 반전처리 방안1, 2와 제안방안의 결과 비교

제안된 방안은 반전 위치가 랜덤하고, 균일하기 때문에 출력 난수열의 패턴에 종속적이지 않다. 그러므로 주어진 유의수준을 만족하는 값을 얻을 수 있었다.

런 검증항목은 한 사이클(20000비트) 가운데 "1" 비트 수가 연속되는 비트의 최대 시퀀스를 런이라 정의하고, 이때 "1"비트 수가 연속적으로 1부터 6까지 발생되는 런 수를 합한 값이 주어진 유의수준을 만족하면 검증을 통과하는 것으로 판정한다. 편이성이 심한 출력 난수열의 경우 런의 길이가 특정길이에 종속되어 나타난다. 출력 난수열의 특성에 따라 다르겠으나 실험된 데이터의 경우 런의 길이가 3일 경우 특히 많은 비트가 존재하는 것을 볼 수 있다. 런의 길이를 1부터 6까지 검사해보면 방안1과 방안2의 경우 주어진 유의수준 값에서 벗어나는 값을 갖는 반면 제안된 방안은 유의수준 범위를 만족하는 것을 확인할 수 있었다.

## 5. 결 론

하드웨어 부품으로만 구성된 실난수 발생기는 출력 난수열이 편이성을 갖지 않는 통계적 랜덤성(randomness)을 제공하는데 한계가 있다. 그러므로 실난수 발생기에 해쉬함수나 LFSR 결합모델을 사용한다. 그러나 기존의 제안된 모델에서 제공된 난수열의 랜덤성(randomness)은 해쉬함수나 LFSR의 비도에 의존하게 되므로, 실난수 발생기가 제공하는 비주기적인 특성을 제한하는 결과를 초래한다. 특히 소프트웨어로 구현된 LFSR 결합모델은 여전히 추측이 불가능한 시드(seed) 값 관리라는 문제를 안고 있다. 따라서 하드웨어로 구현된 출력 난수열이 안정화된 실난수 발생기가 요구된다. 본 논문에서는 편이성을 갖는 출력 난수열에

대해 주어진 1 사이클 동안 출력 난수열 "0"과 "1" 비트의 분포를 파악하고, 출력 비트의 듀티 정보를 이용하여 출력 난수열을 안정화시킴으로써 편이성을 갖지 않는 출력 난수열을 얻도록 하였다. 출력 난수열을 안정화 시키는 방안으로서 주어진 기간동안 전체 출력 난수열 가운데 "1"비트의 밀도분포를 파악하고 분포가 0.5의 값을 갖도록 유도하였다. 이때 안정화된 출력 난수열은 편이성을 갖는 출력 난수열에 비해 FIPS 140-1에서 제시하는 난수발생기의 랜덤성(randomness) 검증 조건을 만족하는 것을 확인하였다.

## 참고문헌


[1] C. S. Petrie and J. A. Connelly, "A Noise-Based Random Bit Generator IC for Applications in Cryptography", Proc. ISCAS '98, June 1998.

[2] http://www.io.com/~ritter/RES/NOISE.HTM.

[3] http://www.clark.net/pub/cme/P1363/ranno.html.

[4] http://webnz.com/robert/true_rng.html.

[5] J. Von Neumann, "Various techniques used in connection random digits", Nat. Bur. Stand. Appl. Math. Ser., Vol. 12, pp. 36-38, 1951.

[6] FIPS 140-1, "Security Requirements for Cryptographic Modules", [Federal Information Processing Standards Publication 140-1], U.S. Department of Commerce/NIST[National Technical Information Service] Springfield, Virginia, 1994. http://ncsl.nist.gov/fips/ fips1401.htm.

[7] Douglas R. Frey, "Chaotic Digital Encoding: An Approach to secure communication", Analog and Digital Signal Processing, Vol. 40, No. 10 Oct., pp. 660-666, 1993.

[8] L. Kocarev, K. Halle, K. Eckert, and L.Chua, "Experimental demonstration of secure communications via chaotic synchronization", Int. J. Bifurcation Chaos, Vol. 2, pp. 709-713, Sep. 1992.

[9] Henry D. I. Abarbanel and Paul S. Linsay, "Secure Communications and Unstable Periodic Orbits of Strange Attractors", IEEE Trans on circuits and system, Vol. 40, No. 10, Oct. 1993.

[10] G. M. Bernstein and M. A. Lieberman, "Secure Random Number Generator Using Chaotic Circuits" IEEE, May 1989, pp. 640-644.

[11] L. M. Pecora and T. L. Carroll, "Driving systems with chaotic signals", Phys. Rev. A, Vol. 44, pp. 2374-2383, Aug. 1991.

[12] U. Parlitz, L. O. Chua, L. Kocarev, K. S. Halle, and A. Shang, "Transmission of digital signals by chaotic synchronization", Int. J. Bifurcation chaos, Vol. 2, pp. 973-977, 1992.

[13] M. E. Bianco and D. A. Reed, Encryption System Based on Chaos Theory, US Patent No. 5, 048,086, Sep. 10, 1991.

[14] Matto B, Caudio N, Pietro P, and Dario P, "A noise model for digitized data", IEEE trans. on instrumentation and measurement, Vol.49, No.1, pp. 83-86, Feb. 2000.

[15] C. S. P and J. A. C, "A noise based IC random number generator for applications in cryptography", IEEE trans. on circuits and systems-1:fundamental theory and applications, Vol.47, No.5, pp. 615-621, May 2000.