Journal of the Korea Academia-Industrial cooperation Society
Vol. 13, No. 2 pp. 755-759, 2012

http://dx.doi.org/10.5762/KAIS.2012.13.2.755

하드웨어 잡음원 기반의 난수발생기의 사후처리 특성 분석

홍진근[1*]
[1]백석대학교 정보통신학부

Analysis of Post Processing Characteristics of Random Number Generator based Hardware Noise Source

Jin-Keun Hong[1*]
[1]**Division of Information Communication, Baekseok University**

요 약 본 논문에서는 의학, 게임분야에서 활용되는 하드웨어 기반의 난수 발생기에 관한 것이다. 인텔은 하드웨어 기반 실난수 발생기의 보안성에 대한 가이드라인을 제시한 바 있다. 주로 존슨 열 잡음원을 사용하며, 듀얼 오실레이터나 폰 노이만 수집기를 적용하고 있다. 하드웨어 기반의 난수 발생기는 NIST 통계검정, FIPS140-1을 포함한 다양한 테스트 유형을 적용하고 있다. 본 논문에서는 하드웨어 잡음원의 출력열에 필터링 기법 영향으로부터 난수성 변화 정도를 측정하였다.

Abstract In this paper, it is about random number generator, which is based on hardware is utilized in medical science and game area. The Intel presents guideline of security level about hardware based true random number generator. At hardware based random number generator, the various test items, that are included in test suits as NIST statistical test, FIPS140-1, is applied. In this paper, it experiments about degree extent of randomness variation from filter scheme effects, which is applied in output stream of hardware noise source.

Key Words : Noise, Random, Security level

1. 서론

키수열을 생성하는 실난수 발생기는 통계적인 랜덤성(randomness)을 제공하는 것이 핵심이며, 일반적으로 자연현상으로부터 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. 이러한 발생기는 그 시드(seed) 값이 완전한 랜덤성(randomness)을 제공하는 소스를 필요로 하나, 결정적인 시스템이라는 특성 때문에 완전한 랜덤성(randomness)을 제공하는 소스를 생성시키는 것이 현실적으로 불가능하다.

비결정적인 출력난수를 제공하는 실난수 발생기의 경우 동일하게 보편적인 하드웨어를 사용하는데, 그 특성상 속도가 느리고, 구현이 어렵기 때문에 난수 성능이 보장되지 않는 하드웨어라는 전제를 필요로 한다. 본 논문은 이러한 실난수 생성의 한계점들을 고찰하고, 키수열의 사후처리 과정에 요구되는 필터처리 방식에 대해 고찰하였다. 특히 고주파 필터나 라플라시안 필터 처리와 같은 방식을 출력열에 적용해 봄으로써 난수성에 어떤 영향을 받게 되는지를 살펴보았다. 본 연구의 필요성은 의학 분야나 게임분야에서 많이 활용되고 있는 난수발생기의 경우, 순수한 하드웨어 기반의 출력수열만을 활용하기보다 일정수준 이상의 난수성 보장을 목적으로 소프트웨어 필터를 결합하여 구성하는 방안에 대한 연구가 필요하다. 이런 측면에서 본 연구는 활용성 측면에서 그 연구 의의를 가진다. 기존 연구에서는 하드웨어 기반의 잡음원 발생기에 대한 다양한 연구가 수행되었다[1-7]. Matteo Bertocco 등[8]은 디지털 데이터를 위한 잡음 모델이라는 연구에서 잡음 양자화기, 잡음 디지타이저의 간략화 모델에 대한 연구에 초점을 맞춘 바 있다. Fabrizio Cortigiani 등[9]은 하드웨어 기반의 실난수 발생기의 고속화 모델에 대해 연구를 수행하였으며, MOS 구

*교신저자 : 홍진근(jkhong@bu.ac.kr)
접수일 11년 12월 21일 수정일 12년 02월 02일 게재확정일 12년 02월 10일

조의 특성을 주제로 접근한 바 있다. Ki-Cheo Tae 등[10]은 DCT 기반의 잡음 발생 시스템에 대해 연구를 수행한 바 있고, Jean Luc Danger 등[11]은 통신채널에서 가우스 잡음 발생기의 효율적인 FPGA 구현이라는 주제에 관심을 가지고 연구한 바 있다. 이 연구에서는 FPGA 최적화에 대한 접근하고 있다. Bruno Ando 등[12]은 트랜스 듀서에 잡음 생성을 위한 CNN에 대한 연구에 대해, Santina Rocchi 등[13]은 카오스적인 CMOS 실난수 A/D 백색 잡음 발생기에 대한 관심을 가지고 연구하였다. 이 연구에서 발생기 구조는 오프셋 튜닝부, 트랜스컨덕턴스 증폭부, Gm 튜닝부, 전류원부, 비교기, 트랜스 임피던스 증폭부로 구성되고 있다.

본 논문의 구성은 2장에서 하드웨어 잡음원 발생기의 구성과 이 발생기의 난수성을 평가하는 항목들에 대해 살펴보고, 3장에서 필터링 기법이 적용된 하드웨어 기반의 잡음원 발생기에 대해, 4장에서 실험결과를 고찰하고, 5장에서 결론을 맺었다.

2. 하드웨어 잡음원 기반의 난수발생기

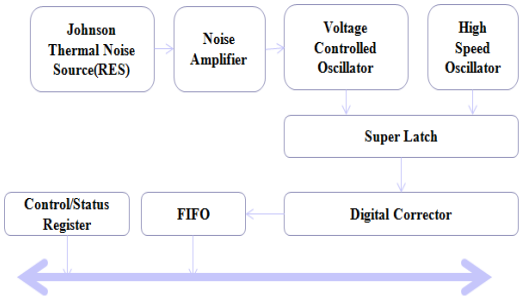
하드웨어 발생기에 적용되는 잡음원은 백색 가우스 잡음으로서 주어진 대역폭에 비례하는 잡음전력을 갖는다. 가우스 잡음은 가우스 진폭분포를 갖는다. 가우스 잡음 분포함수 $f(x)$ 의 확률밀도는 식(1)에서와 같이 정의할 수 있다.

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

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

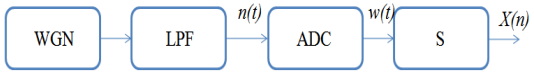
2.1 하드웨어 잡음원 발생기 구성

일반적으로 하드웨어 기반의 잡음 발생기는 디지털 필터부, 디지털 인터페이스 회로, DAC, 아날로그 필터, 출력부로 조합된다. Craig S. Petrie의 연구에서는 잡음 발생기 구성을 잡음원, 증폭기, VCO, 1/x 출력부 등으로 조합하기도 하는데, 이러한 구조에서는 안정된 잡음원이나 안정화된 발진기의 사용이 핵심적인 요소로 고려된다.



[그림 1] 인텔의 발생기 구조도
[Fig. 1] Generator Structure of Intel

TRNG(True Random Number Generator)의 구성은 백색가우시안잡음(WGN), LPF(low pass filter), ADC (comparator), S(sampler)로 이루어진다. 잡음원은 아날로그 전자 회로로 대역 제한된 WGN에 근사화 되며, 샘플링을 처리하기 이전에 이산 처리된다. 이어 양자화, 비교화 등의 방법으로 디지털로 변환된다. 컨버터와 샘플러는 WGN 소스로부터 난수성을 추출한다. 디지털화된 잡음은 먼저 잡음원을 추출하고 디지타이저로 디지털화 처리한다. 디지털화된 신호는 사후처리 알고리즘을 통하고 인터페이스를 거쳐 난수를 발생하게 된다. 또한 디지털 처리된 잡음 신호는 엔트로피 추정자를 통해 낮은 엔트로피를 갖는 난수열에 대해 경고한다. 낮은 엔트로피는 암호학적 요구조건을 만족시킬 수 없다.



[그림 2] TRNG 간략화된 구조도
[Fig. 2] Simplified Structure of TRNG

2.2 하드웨어 잡음원 평가 항목

일반적으로 적용되는 평가항목으로 인텔의 통계적인 평가 방안은 블록 평균 스펙트럴 분석, 랜덤 워크 테스트, 블록평균, 주기성, 스펙트럴 분석, 자기상관성, 8비트와 16비트 Maurer /monkey /goodness of fit 테스트, 런검정, FIPS 140-1 테스트 등이 적용된다. 미정부 기관인 NIST는 SP800-90 결정적 랜덤 비트 발생기의 승인시스템을 정의하고 있으며(2009, Revised), FIPS PUB 140-2에서는 암호모듈을 위한 보안 요구조건을 정의하고 있다. 또한 SP800-90에서는 해쉬_DRBG, HMAC_DRBG, CTR_DRBG, Dual_EC_ DRBG에 대한 테스트를 실시한다. 하드웨어 기반의 난수발생기에 대한 연구, 이를 검증하기 위한 테스트 방안도 적용된다. 스탠포드대학은 Semi

numerical 알고리즘(주기성, 시리얼, 갭, 포커, 쿠폰 콜렉터, 치환, 런, 최대 충돌성, 생일 스페이싱, 시리얼 상관성)이 적용되며, 플로리다대학에서는 다이하드(birthday spacings, overlapping permutations, ranks of 31x31 and 32x32 matrices, ranks of 6x8 matrices, monkey tests on 20-bit Words, monkey tests OPSO, OQSO, DNA, count the 1's in a stream of bytes, count the 1's in specific bytes, parking lot, minimum distance, random spheres, squeeze, overlapping sums, runs, craps) 방식이 주를 이룬다. 또한 퀸스랜드 대학은 Crypt-XS(frequency, binary derivative, change point, runs, sequence complexity and linear complexity), CRC 프레스 인코퍼레이션사에서는 응용 암호학 핸드북(frequency, binary derivative, change point, runs, sequence complexity and linear complexity)을 기반으로 한다. NIST ITL의 NIST 통계적인 테스트 슈트는 frequency, block frequency, cumulative sums, runs, long runs, Marsaglia's rank, spectral (based on the Discrete Fourier Transform), nonoverlapping template matchings, overlapping template matchings, Maurer's universal statistical, approximate entropy (based on the work of Pincus, Singer and Kalman), random excursions(due to Baron and Rukhin), Lempel-Ziv complexity, linear complexity, and serial) 등이 주로 사용되어 오고 있다.

이러한 평가 방안들은 문턱치, 고정된 범위, 확률 값을 중심으로 평가하며, NIST의 경우, 단일 이진 시퀀스에 대해 단계별로 평가가 이루어지고 있다. 이 평가항목은 널 가정, 시퀀스 테스트 통계, P 값 계산, P 값 범위 비교에 대해 시행된다. 통계 테스트는 주기성, 누적 합, 런 검정(제일 긴 1의 수), 런, 랭크, 스펙트럴, 오버랩 되지 않은 템플릿 매칭, 오버레핑된 탬플릿 매칭, 유니버설 통계, 랜덤성 유지, 랜덤성 유지 변동폭, 근사 엔트로피, 시리얼, Lempe1-Ziv 복잡도, 선형복잡도 항목을 기반으로 난수성 평가 검증이 이루어지고 있는 실정이다. 본 논문에서는 주요 평가지수로, Frequency, serial, poker를 주요 평가지수로 사용하였다.

3. 사후처리 기법이 적용된 하드웨어 잡음원 발생기

필터가 주로 사용되는 사후처리기법은 잡음원의 불완전성을 제거할 목적으로 사용되며, 디지털화된 잡음 신호의 압축 함수를 적용하여 난수 비트의 엔트로피성을 증가시킨다. 이와 같은 방법에는 폰 노이만 교정기, XOR 교정기, 해시 함수나 탄성함수 등이 주로 사용된다. 물론 현실적으로 플립플롭 홀드조건이나 셋업 조건의 위반에 따라 플립플롭 내부 게이트 쌍이 논리적으로 high/low 상태가 아닌 중간상태로 예측되지 않은 방향으로 발진 등과 같은 메타 안정성과 같은 문제가 일어날 수 있다.

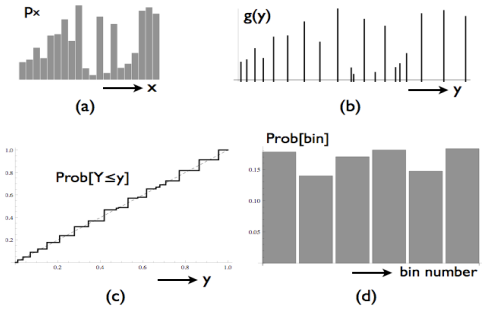
3.1 잡음원의 이산 처리 분포 특성

일반적으로 적용되는 이산분포는 다음 식과 같은 특성을 지닌다.

$f(x)=\sum_{i=1}^{n} p_i \delta(x-x_i)$ 이며,

$Y=\sum_{i=1}^{n} p_i \Theta(X-x_i)$ 의 조건이 주어질 때,

다음과 같은 분포 특성을 지닌다.

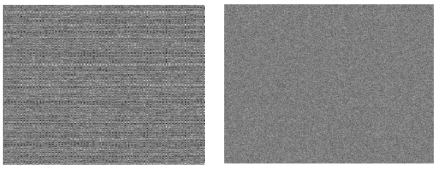


[그림 3] 이산 랜덤함수의 분포도
[Fig. 3] distribution degree of discrete random function

여기서 (b)는 비균일 분포(non uniform), (c)균일분포(uniform)의 cdf 특성으로 근접한다. 또한 (d)에서 거의 0.15를 중심으로 유사한 분포 특성을 가지는 것을 알 수 있다.

3.2 잡음원의 필터 처리 사례

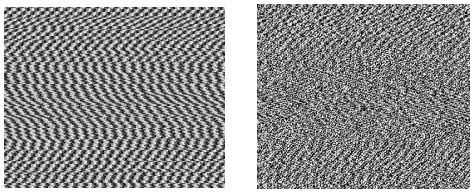
일반적인 필터 기법 사례로 FFT를 들 수 있다. FFT가 처리이전과 처리후 백색잡음(White Gaussian)의 사후처리 패턴은 다음과 같다.



(a) 미처리 (b) FFT처리
(a) No processing (b) FFT processing

[그림 4] 백색 잡음의 사후처리
[Fig. 4] Post processing of WG

다음은 고주파 필터링 처리된 잡음원의 사후처리 예를 제시한 것이다.



(a) 미처리 (b) 2차고주파필터처리

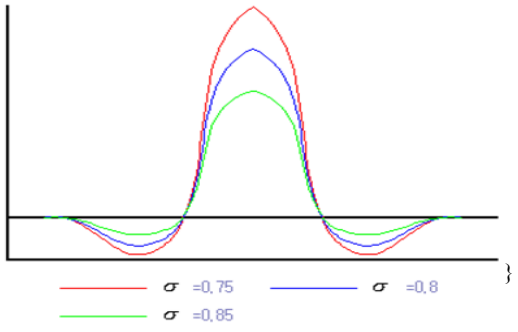
(a) No processing (b)2nd HPF processing

[그림 4] 백색 잡음의 고주파 필터 사후처리
[Fig. 4] HPF posting processing of WG

3.3 가우시안 필터 함수의 사례

```
int x,y,p,q,div;
// 가우시안 필터
int sum, Gaussian[3][3]={{1,2,1},{2,4,2},{1,2,1}};
int filter1[7][7] = {{0,0,-1,-1,-1,0,0}, {0,-2,-3,-3,-3,-2,0},
{-1,-3,5,5,5,-3,-1},
{-1,-3,5,16,5,-3,-1}, {-1,-3,5,5,5,-3,-1}, {0,-2,-3,-3,-3,-2,0},
{0,0,-1,-1,-1,0,0}};
div = 0;
for(q=0; q<=2; q++){
for(p=0; p<=2; p++){
div = div + Gaussian[q][p];
}
```

2차 가우시안 라플라스 함수 도식을 다음 그림5에서 제시하였다.



[그림 5] 2차 가우시안 라플라스 함수
[Fig. 5] 2nd Gaussian Laplace function

식2에서는 2차 가우시안 라플라스 함수를 나타낸 것이다.

$$f(x) = \frac{1}{\pi\sigma^4}\left[1 - \frac{x^2+y^2}{2\sigma^2}\right] e^{\frac{-(x^2+y^2)}{2\sigma^2}} \quad (2)$$

4. 실험결과

4.1 고주파 필터 적용에 따른 난수성 영향

다음 표1에서는 고주파 필터 방식과 난수성 결과를 비교한 것이다. 하드웨어 잡음원(원본)이 고주파 필터(2차, 3차, 4차, 차, 6차) 적용에 따라 난수성의 정도에 영향을 주고 있음을 확인할 수 있으며, 차수의 정도에 따라 난수성에 어떤 영향을 주는지 파악할 수 있다.

하드웨어 잡음원은 고주파 필터 처리보다 라플라시안 함수에 의한 필터 처리방식에서 난수성 영향이 비효율적임을 파악할 수 있다. 특히 라플라시안 필터의 5차에서 보다 효율적임을 파악할 수 있다.

[표 1] 고주파 필터 방식과 난수성 결과 비교
[Table 1] Comparison of HPF method and Randomness Result

난수성 검증시험	잡음원	HPF (2차)	HPF (3차)	HPF (4차)	HPF (5차)	HPF (6차)
frequency	4208	1442	478	957	660	6608
serial	4285	2046	742	1267	906	5638
3-serial	6333	3223	1142	1909	1601	8684
4-serial	16178	53111	1834	3316	2468	24211
5-serial	25456	7214	2702	4262	3467	61404
poker-3	4943	2243	786	1368	1024	6610
poker-4	31495	6841	2048	4583	3164	36063
poker-5	11293	3872	1386	2336	1806	19096

[표 2] 라플라시안 필터 방식과 난수성 결과 비교
[Table2] Comparison of Laplacian filter method and Randomness Result

난수성 검증시험	잡음원	2차	5차	7차
frequency	4208	1255	35	8897
serial	4285	1964	68	13063
3-serial	6333	3144	87	20662
4-serial	16178	5067	133	32062
5-serial	25456	7317	184	45046
poker-3	4943	2125	65	14198
poker-4	31495	5646	166	3688
poker-5	11293	3761	101	23953

상기 분석을 통해, 하드웨어 잡음원 기반의 수열 발생기는 고주파 필터 적용방식보다 라플라시안 필터 적용방식에서 난수성 정도에 보다 효율적임을 확인할 수 있었다. 라플라시안 필터 함수에서 5차를 적용할 경우 보다 효과적임을 알 수 있다.

5. 결 론

본 논문에서는 하드웨어 잡음원을 생성하는 실난수 발생기에서 통계적인 랜덤성의 안전성을 보장이라는 이슈를 위해 사용되는 필터 사후처리 기법에 대해 고찰하였다. 비결정적인 출력난수를 제공하는 실난수 발생기가 보다 안정적인 출력 수열을 제공하기 위해 제공되는 사후처리 기법을 고주파 필터, 라플라시안 필터를 통해 어떤 영향을 난수성 측면에서 받는지를 살펴보았다. 본 연구는 의학 분야나 게임 분야에서 많이 활용되고 있는 난수발생기가, 순수한 하드웨어 기반의 출력수열에 소프트웨어 필터를 결합모델로 구성함으로써 일정 수준 이상의 난수성을 보장할 수 있도록 한다. 본 연구는 실제 활용되는 하드웨어 발생기 설계 측면에 보다 효용성을 가질 것으로 사료된다. 또한 향후 하드웨어 잡음원 모듈과 소프트웨어 필터 방식 결합모델의 소형화 이식에 대한 연구를 하고자 한다.

References

[1] Michal Varchola, FPGA Based True Random Number Generators for Embedded Cryptographic Applications, Thesis of PhD, Technical University of Kosice, 2008.

[2] M. Dichtl and J. Golic, "High-speed true number generation with logic gates only,"in Cryptographic Hardware and Embedded Systems - CHES 2007, Vienna, Austria, September 10-13, 2007, Proceedings, ser. LNCS, vol. 4727. Springer, 2007, pp. 45-61.

[3] V. Fischer, A. Aubert, B. Valtchanov, and N. Bochard, "True random number generators in congurable logic devices,"September 2008, processing.

[4] P. Lacharme, "Post-processing functions for a biased physical random number generator,"in Fast Software Encryption workshop - FSE 2008.

[5] E. Barker and J. Kelsey, "Nist special publication 800-90: Recommendation for random number generation using deterministic random bit generators," National Institute of Standards and Technology (NIST), Computer Security Division Information Technology Laboratory, March 2007.

[6] B. Valtchanov, A. Aubert, F. Bernard, and V. Fischer, "Modeling and observing the jitter in ring oscillators implemented in fpgas,"in The 11-th IEEE Workshop on Design and Diagnostics of Electronic Circuits and Systems (DDECS), Bratislava, April 2008, pp. 158-163.

[7] V. Fischer, F. Bernard, N. Bochard, and M. Varchola, "Enhancing security of ring oscillator based rng implemented in fpga,"in Field-Programable Logic and Applications (FPL), September 2008, pp. 245-250.

[8] Bertocco, M. Narduzzi, C. Paglierani, P. Petri, "A noise model for digitized data," IEEE transactions on Instrumentation and Measurement, Vol.49, Issue 1, pp.83-86, 2000.

[9] Ada Fort, Fabrizio Cortigiani, Santina Rocchi, Valerio Vignoli, "Very High Speed True Random Noise Generator," Kluwer Academic Publisher. AICSP2003, 34, pp.97-105, 2003.

[10] Ki-Cheol Tae, Jin-Gyun Chung, Dae-Ik Kim, "Noise generation system using DCT," ISCAS 2001, pp.29-32, 2001.

[11] Danger J. L., Ghazel A., Boutillon E., Laamari H., "Efficient FPGA implementation of Gaussian noise generator for communication channel emulation," ICECS2000, Vol.1, pp.366- 369, 2000.

[12] B. Andò, S. Graziani, Stochastic Resonance: Theory and Applications, Kluwer academic publishers, 2000.

[13] Santina Rocchi, Valerio Vignoli, "A Chaotic CMOS true random analog/digital white noise generator," ISCAS1999, pp.463-466, 1999.

홍 진 근(Jin-Keun Hong) **[정회원]**

- 2012년 2월 현재 : 백석대학교 정보통신학부 교수

<관심분야>
전술통신, 센서넷, RFID, 무선랜 보안