ISSN : 1226-7244 (Print)
ISSN : 2288-243X (Online)
논문번호 20-02-25
172

j.inst.Korean.electr.electron.eng.Vol.24,No.2,543~549,june 2020
http://dx.doi.org/10.7471/ikeee.2020.24.2.543

최신 준안정성 및 발진기 기반 진 난수 발생기 비교

Comparison on Recent Metastability and Ring-Oscillator TRNGs

신 화 수*, 유 호 영*★

Hwasoo Shin*, Hoyoung Yoo*★

Abstract

As the importance of security increases in various fields, research on a random number generator (RNG) used for generating an encryption key, has been actively conducted. A high-quality RNG is essential to generate a high-performance encryption key, but the initial pseudo-random number generator (PRNG) has the possibility of predicting the encryption key from the outside even though a large amount of hardware resources are required to generate a sufficiently high-performance random number. Therefore, the demand of high-quality true random number generator (TRNG) generating random number through various noises is increasing. This paper examines and compares the representative TRNG methods based on metastable-based and ring-oscillator-based TRNGs. We compare the methods how the random sources are generated in each TRNG and evaluate its performances using NIST SP 800-22 tests.

요 약

산업의 발전과 인터넷의 발전으로 보안의 중요성이 증가하면서 암호화에 필수적인 요소인 암호화 키의 생성에 사용되는 난수 발생기의 연구가 활발하게 이루어지고 있다. 외부 공격으로부터 안전한 고성능의 암호화 키를 생성하기 위해서는 예측하기 어려운 품질 좋은 난수 발생기가 필수적이다. 일반적으로 사용되는 의사 난수 발생기는 충분한 성능의 난수를 발생하기 위해서 많은 양의 하드웨어 리소스가 요구됨에도 외부에서 암호화 키를 외부에서 알아낼 가능성이 존재한다. 그러므로, 다양한 잡음을 통해 난수를 발생시켜 외부에서 예측 불가능하며 품질 좋은 진 난수 발생기에 대한 요구가 증가하고 있다. 본 논문은 진 난수 생성기술로 대표적인 준안정성 및 발진기를 통한 진 난수 발생기의 최신구조가 랜덤소스를 생성하는 방식을 조사 및 비교한다. 또한, NIST에서 제공하는 난수 검증용 도구인 SP 800-22 테스트를 통해 발진기 기반 진 난수 발생기 성능을 검증한 자료를 분석한다.

Key words : True Random Number Generator, Metastability, Ring Oscillator, Encryption, Encryption key

* Dept. of Electronics Engineering, Chungnam National University
★ Corresponding author
E-mail : hyyoo@cnu.ac.kr, Tel : +82-42-821-6585

※ Acknowledgment
This work was supported by the Brain Korea 21 Plus and by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (NRF-2019M3F3A1A01074449)
Manuscript received Jun. 1, 2020; revised Jun. 23, 2020; accepted Jun. 24, 2020.

Ⅰ. 서론

산업의 발전이 이루어지면서 모든 기업, 연구소와 같은 단체들의 보안에 대한 중요성이 부각되었고, 또한, 인터넷의 발전으로 은행 업무, 소셜 네트워크 서비스 등의 사용자가 나날이 증가하면서, 개인에 대한 중요 개인정보의 유출은 심각한 사회적 문제로 대두되고 있다. 이를 위해 다양한 보안 솔루션이 개발되었으며, 대표적으로 암호화 키를 이용한 암호화 방식이 폭넓게 사용된다. 암호화 키를 이용한 암호화 방식은 암호화 키를 외부에서 유추할 수 없도록 생성하는 것이 핵심이며, 이 암호화 키를 생성하기 위해 일반적으로 사용되는 기술이

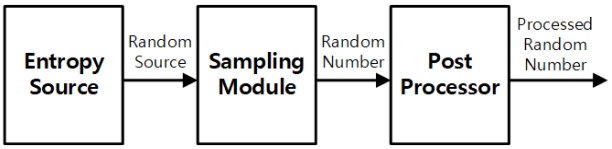

Fig. 1. Representative structure of TRNGs.
그림 1. 진 난수 발생기의 대표구조

난수 생성기술이다. 난수 생성기술을 통해 암호화 키를 생성하고, 생성된 암호화 키의 성능을 높이기 위해서는 품질 좋은 난수의 생성이 필요하다. 난수 생성기술은 의사 난수 생성기술과 진 난수 생성기술로 나뉘는데, 초기의 암호화 키 생성은 비교적 구현이 단순하고 쉬운 의사 난수 생성기술을 이용했다. 그러나 의사 난수 생성기술은 출력의 예측이 가능하므로 외부에서 암호화 키를 알아내어 보안 문제를 일으킬 염려가 있으므로, 최근 진 난수 발생기의 연구 및 개발이 활발하게 이루어지고 있다.

일반적으로 사용되는 하드웨어 의사 난수 생성기는 선형 피드백 시프트 레지스터와 같은 구조를 이용하여 구성된다[1]. 이러한 구조로 인해 의사 난수 발생기는 온전한 난수가 아닌 일정 범위 안의 값을 정해진 순서에 맞추어 출력하는 선형성을 갖게 되지만, 통계학 입각 기준에 따라 일정 수준 이상의 의사 난수를 난수로 가정하여 사용하게 된다. 하지만 이 경우, 외부의 공격자가 난수의 발생 패턴을 유추할 가능성이 존재하기 때문에 출력의 범위를 최대한 늘려서 유추하기 어렵도록 구현해야 하지만, 출력의 길이가 길어질수록 하드웨어 오버헤드의 증가가 불가피하다. 이러한 의사 난수 발생기의 예측 가능성을 보완하기 위해 진 난수 발생기의 개발이 활발하게 이루어지고 있다. 진 난수 발생기는 다양한 종류의 잡음원을 이용하여 특정 회로에 랜덤성을 부여하고, 이를 통해 예측 불허한 출력을 생성한다. 일반적으로 진 난수 생성기술은 PLL(Phase-Locked Loop) 방식, Self-Timed Ring 방식, Metastability (준안정성) 방식[2-4], 그리고 Ring Oscillator (발진기) 방식[5-9]으로 크게 4가지 방식을 통해 랜덤소스를 생성한다[1]. 진 난수 발생기는 그림 1에서 보이는 바와 같이 각 랜덤소스를 구현하기 위한 하드웨어, 출력된 랜덤 소스를 난수로 변환하기 위한 샘플링, 그리고 의미 있는 난수 생성을 위한 후 처리 하드웨어[10-11]로 구성되기 때문에 상대적으로 적은 하드웨어 오버헤드를 사용하여 구현할 수 있다[1-9]. 본 논문에서는 다양한 방식으로 연구 및

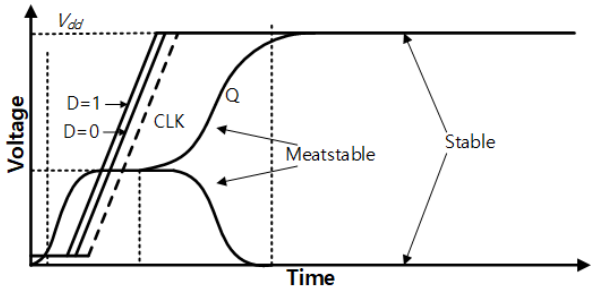

Fig. 2. Metastable voltage condition.
그림 2. 준 안정 상태의 전압

개발되고 있으며 구현 난이도와 성능 측면에서 선호되어 일반적으로 많이 사용되는 준안정성 기반[2-4] 및 발진기 기반[5-9]의 진 난수 발생기를 연구한 논문을 분석한다.

II. 본론

1. 준안정성 기반 진 난수 발생기

준안정성은 CMOS 회로에서 pull-up과 pull-down 회로가 모두 부분적으로 동작하여 low도 아니고 high도 아닌 중간상태를 지속하는 현상으로 일반적인 하드웨어 설계에서 준안정성 현상의 발생은 회로의 동작을 방해하여 정상적인 출력의 생성을 위해서는 회피해야 한다[2-4]. 준안정성은 그림 2에서 보이는 바와 같이 전압의 크기가 안정적이게 되는 V_{dd}와 GND의 중간 부근의 값을 갖게 되어 불안정한 상태를 형성한다. 특정 모듈에서 준 안정 상태가 유지되면 회로의 출력은 한 값으로 결정되지 않고, 알 수 없는 값이 출력되므로 이후의 모듈에서 값을 인지할 수 없어 전체적인 출력이 정상적으로 생성될 수 없게 된다. 그러나 준안정성을 기반으로 하는 진 난수 생성기술은 의도적으로 high 또는 low로 결정되지 않은 준안정성 상태를 유도하여 불안정한 출력을 생성하다가 회로에 다양한 잡음으로 랜덤성을 부여하여 준 안정 상태의 회로가 임의의 한 값으로 결정되도록 하는 방식을 통해 난수를 생성한다.

[2]는 준안정성 기반의 진 난수 발생기에 대한 구조를 제안하고 있다. 이 논문에서는 그림 3에서 보이는 것과 같이 MUX를 이용하여 인버터의 입력이 클록에 맞추어 변화되면서 Metastability(MS) 모드와 Generation(Gener.) 모드가 반복되며 생기는 변화가 진 난수 발생기의 랜덤소스로 사용된다. MS

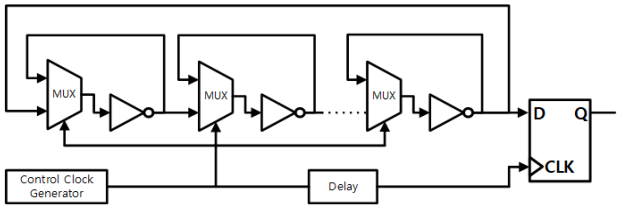

Fig. 3. Metastability-based TRNG[2].
그림 3. 준안정성 기반 진 난수 발생기[2]

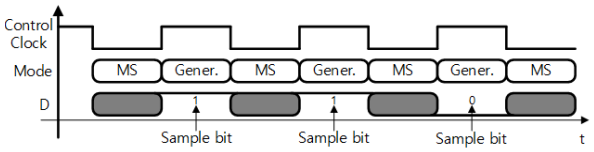

Fig. 4. Metastability-based TRNG timing diagram[2].
그림 4. 준안정성 기반 진 난수 발생기 타이밍도[2]

모드는 준 안정 모드를 의미하며, 그림 4에서 보이는 바와 같이 클록이 low일 때, 각 단의 인버터 출력이 MUX에 의해 입력으로 피드백되어 각 인버터가 준 안정 상태가 된다. 이때의 출력은 준 안정 상태이므로 알 수 없는 값이 출력되어 정상적인 동작이 불가능하지만, 클록이 high로 변화하면서 Gener. 모드가 되면 각 단의 인버터 출력이 MUX에 의해 다음 단의 인버터 입력으로 들어가면서 잡음의 영향을 받아 난수를 출력하게 된다. 랜덤소스에서 출력된 난수는 지연 모듈을 거친 클록에 의해 DFF에서 샘플링되어 폰 노이만 후처리 모듈[10-11]로 입력된다. 폰 노이만 후처리 방식은 대부분의 진 난수 발생기에서 선호되는 방식으로, 출력이 00과 11일 때는 제거하고 10일 때는 1, 01일 때는 0으로 대입하여 출력을 조정한다. 후처리를 거친 출력은 비록 그 길이가 입력 대비 25% 수준으로 감소하지만, 연속 시퀀스를 제거함으로써 0과 1의 비율을 유사하게 조정한다.

2. 발진기 기반 진 난수 발생기

발진기는 홀수개의 인버터를 체인 형태로 연결하여 연결된 인버터의 개수만큼의 딜레이를 갖고 홀수개의 인버터를 거쳐 입력이 반전되어 출력되며 일정 주기를 갖는 펄스를 생성한다[5-9]. 발진기 기반의 진 난수 생성기술은 일반적으로 발진기를 랜덤소스로 활용하여 발진기의 출력을 DFF의 입력 또는 클록 신호로 넣어주는 방법을 통해 샘플링하여 난수를 생성한다. 발진기 기반의 난수 생성기술은 발진기 출력이 잡음의 영향을 받아 클록의 값이

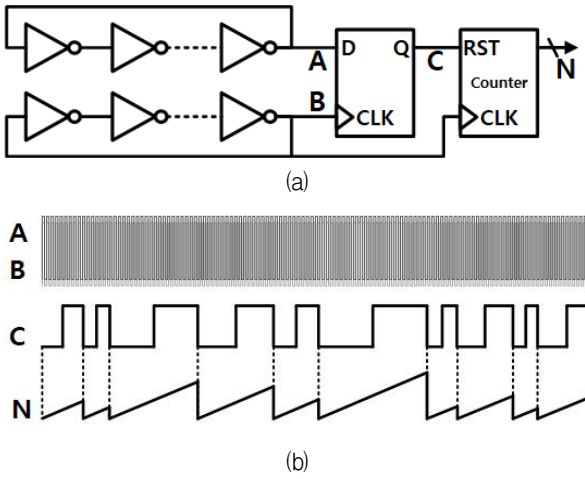

Fig. 5. (a) Beat frequency detection TRNG, (b) BFD TRNG output diagram[5].
그림 5. (a) BFD TRNG의 구조, (b) BFD TRNG 출력[5]

주기보다 빠르게 또는 느리게 변화하여 출력이 불규칙해지는 것이 핵심으로, 지터가 발생하는 정도와 빈도에 따라 난수의 질이 달라진다[5, 6].

[7]은 2개의 서로 다른 발진기를 랜덤 소스로 사용하여 ASIC으로 구현한 발진기 기반 진 난수 발생기에 대한 논문이다. 이 논문에서는 두 개의 발진기를 구현할 때, 두 발진기의 주파수를 약 1% 수준으로 미세하게 차이 나도록 하고, 이 차이를 beat frequency로 정의한다. 이렇게 구현한 두 발진기의 출력은 그림 5-a에서 보이는 바와 같이 샘플링을 위한 DFF의 입력과 클록 신호로 각각 연결되며, 두 발진기 중에서 느린 발진기의 출력이 DFF의 클록 신호로 입력되어 샘플링된다. 다른 난수 발생기와는 다르게 beat frequency 개념을 이용하여 DFF로 출력된 값을 난수로 사용할 수 없으므로, 카운터를 추가하여 한 단계의 샘플링을 더 거치게 된다. 그림 5-b는 클록 지터에 의해 발진기 출력 A와 B가 변하고 DFF에 의해 샘플링된 출력 C의 결과와 카운터를 통해 난수 D가 생성되는 예시를 보인다. 클록 지터가 발생하지 않았을 경우를 생각했을 때, 발진기 A와 발진기 B의 주파수가 1% 차이를 가지면 DFF의 샘플링 과정을 거치면서 기존 발진기의 100 사이클에 해당하는 길이를 갖는 펄스 형태의 출력을 보이게 된다. 여기에 클록 지터가 발생하면서 100 사이클보다 길거나 짧은 길이의 펄스로 출력이 변화하게 되고, 카운터를 통해 이 출력 펄스의 길이를 세어 난수를 생성하게 된다. 생성된 난수는 폰 노이만 후처리 모듈[10,11]을 통해 후처

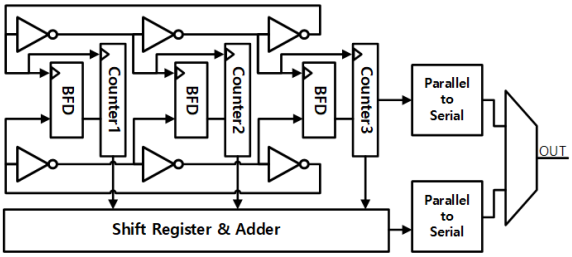

Fig. 6. Multi-stage BFD TRNG[7].
그림 6. 다단 BFD TRNG 구조[7]

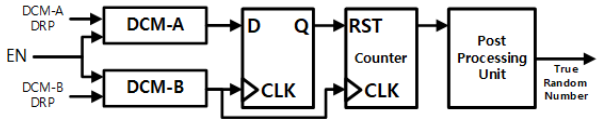

Fig. 7. DCM based BFD TRNG.
그림 7. DCM 기반의 BFD TRNG 구조

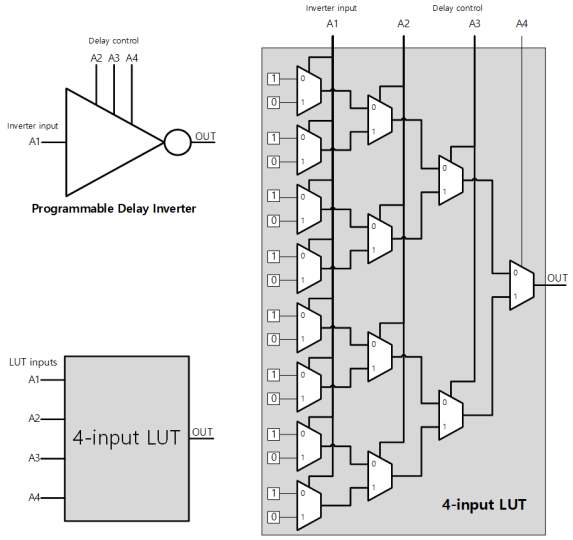

Fig. 8. 4-input LUT based Programmable Delay Inverter[9].
그림 8. 4-입력 LUT 기반의 지연 조절이 가능한 인버터 구조[9]

리 과정을 거치며, 이 후처리 과정에서는 출력 시퀀스를 감소시키는 것이 아닌 기존의 출력 시퀀스에 후처리를 통해 생성된 값을 추가하는 방식으로 동작하여 전체 시퀀스가 증가하도록 설계되었다. 또한, 이 논문에서는 그림 6에서 보이는 바와 같이 동일 회로를 여러 단으로 중첩하는 구조를 제안하고 있으며, 다단 난수 발생기는 발진기를 공유하는 서로 다른 인버터의 출력을 각각 다른 샘플링 모듈로 입력하여 그중 한 단의 출력과 전체를 연산한 출력을 MUX를 통해 선택적으로 사용하는 구조를 갖는다.

[8]은 [7]이 FPGA에 적용하는 과정에서 발진기 회로의 구조 변화로 인해 ASIC에 구현할 수밖에 없었다는 점을 해결하기 위해, 그림 7에서 보이는 바와 같이 발진기를 Xilinx 사의 FPGA 보드 내부에 있는 DCM(Digital Clock Manager) 로 대체하는 방식을 통해 FPGA에 구현하였다.

DCM은 Xilinx 사의 FPGA 보드에 내장되어 있는 보드 내부 클록을 생성하고 조절하는 모듈로 이 논문에서는 DCM에서 생성하는 클록과 클록에 발생하는 클록 지터의 영향을 받아 랜덤 소스로 사용한다. 생성된 랜덤 소스는 DFF를 통해 샘플링하고 카운터를 통해 난수로 변환되어 폰 노이만 후처리 [10, 11] 과정을 거쳐 더 좋은 품질의 난수로 생성된다. ASIC으로 구현된 [7]은 발진기의 주파수가 처음 설정된 값을 유지하지만, DCM을 통해 구현한 발진기는 간단하게 주파수를 조절할 수 있으므로 ASIC 기반의 난수 발생기보다 우수한 활용도를 갖는다. [8]에서는 DCM의 주파수를 다양하게 조절하고 실험하여 난수 생성에 최적화된 두 주파수의 조합을 선정하여 FPGA 보드 내부의 램에 저장하는 방식으로 더욱 편리하게 주파수를 조절하여 난수의 생성을 조절할 수 있다.

[9]는 Xilinx 사의 FPGA 보드를 활용하여 발진기를 구현하여 랜덤소스로 사용하기 위해 PDL (Programmable Delay Line)이라는 개념을 도입하였다. PDL은 Xilinx 사의 FPGA 보드 내부에서 사용되는 4-input 또는 6-input LUT[3]을 이용하여 LUT의 내부에서 데이터의 이동 경로를 선택적으로 사용하여 경로의 차이에 따른 지연시간의 차이를 임의로 조절하는 것이다. 이 논문에서는 그림 8에서 볼 수 있듯이 인버터를 PDL 개념을 활용하여 Programmable Delay Inverter를 구현하여 발진기를 구성하였다. Programmable Delay Inverter는 그림 8과 같이 4-input LUT[3]을 구성하는 MUX tree의 각 MUX 입력을 select 신호와 반대되는 값으로 고정하여 반전 값을 출력할 수 있도록 하고, select 신호 A1을 inverter의 입력으로 설정하여 한 개의 4-input LUT가 한 개의 inverter의 역할을 하도록 구성된다. 입력으로 사용된 A1을 제외한 나머지 3개의 select 신호는 LUT의 출력이 생성되기 위해 거치는 경로를 선택하는 신호로 사용되어 각 경로의 지연시간 차이를 이용하여 inverter의 내부 지연시간을 조절할 수 있도록 한다. 이와 같은 방

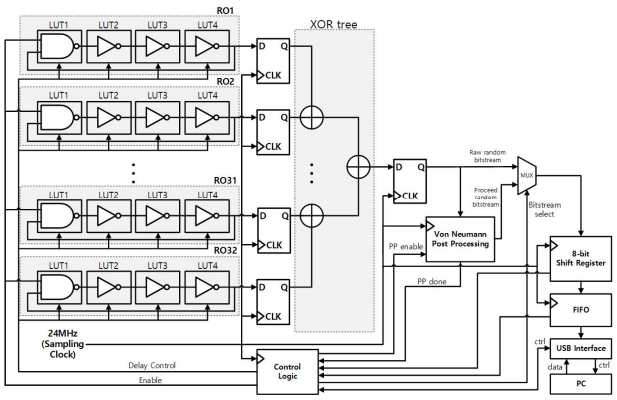

Fig. 9. PDL-based TRNG[9].
그림 9. PDL 기반의 진 난수 발생기 구조[9]

식으로 만들어진 인버터를 그림 9과 같이 체인 형태로 홀수개를 연결하는 방법으로 다수의 발진기를 생성하고, 각 발진기의 인버터에 관하여 입력 및 지연시간 조절에 사용되는 MUX의 select 신호를 컨트롤 로직을 통해 선택적으로 입력할 수 있도록 구성하여 진 난수 발생기의 랜덤소스를 구현한다. 구현된 랜덤소스의 각 발진기에서 생성된 랜덤 비트는 같은 샘플링 클록에 의해 DFF을 통해 샘플링되고, 샘플링된 데이터는 XOR tree를 통한 연산과정을 거쳐 다시 한번 동일한 샘플링 클록으로 DFF에서 샘플링되어 난수로 출력된다. [9]에서는 생성된 난수를 폰 노이만 후처리 모듈[10, 11]을 통해 후처리한 난수와 후처리를 거치지 않은 난수를 MUX를 통해 선택적으로 시프트 레지스터로 입력하여 USB 인터페이스를 통해 PC와 통신할 수 있도록 회로를 구성하여 후처리를 거친 난수 시퀀스와 후처리를 거치지 않은 난수 시퀀스에 대하여 각각 NIST SP 800-22 테스트[12]를 통해 난수성을 비교 검증하였다.

3. 발진기 기반 진 난수 발생기 성능 비교 분석

표 1은 본 논문에서 소개한 발진기 기반 진 난수 발생기의 성능을 NIST에서 제공하는 SP 800-22 테스트[12]를 통해 검증한 결과를 나타내며, 다양한 데이터에 대해 비교한 논문의 경우 한 개의 데이터만을 선별하여 작성하였다. NIST SP 800-22 테스트[12]는 검증하고자 하는 난수 발생기의 출력 시퀀스에 대하여 표 1에 표시한 15가지 항목으로 검증하여 난수 발생기의 난수성을 판단하는 지표로 사용된다. 각 항목의 최소 요건은 p-value가 0.001 이상이어야 하며, 세부적인 성능에 대한 지표는 검사 항목에 따라 달라진다. 각 논문의 성능을 비교하기 위해 Proportion을 확인하였을 때, [7]의 성능이 전반적으로 우수한 값을 보이고 있고, [8]의 경우 Runs와 Nonoverlap.에서 유독 약한 모습을 보인다.

III 결론

본 논문에서는 준안정성 기반의 진 난수 발생기

Table 1. NIST SP 800-22 Test Suite result comparison of Ring Oscillator-based TRNGs.
표 1. 발진기 기반 진 난수 발생기의 SP 800-22 테스트 결과 비교

	[7]		[8]		[9]	
	p-value	Prop.	p-value	Prop.	p-value	Prop.
Frequency	0.514	1.000	0.067	1.000	0.620	0.992
BlockFrequency	0.946	0.982	0.740	1.000	0.744	0.991
CumulativeSums	0.437	1.000	0.122	1.000	0.414	0.987
Runs	0.720	1.000	0.122	0.800	0.428	0.993
LongestRun	0.475	1.000	0.213	1.000	0.701	0.990
Rank	0.055	0.964	0.534	1.000	0.763	0.988
FFT	0.103	1.000	0.534	1.000	0.659	0.994
NonOverlappingTemp.	0.679	1.000	0.009	0.800	0.421	0.993
OverlappingTemplate	0.182	0.982	0.534	1.000	0.081	0.991
Universal	0.063	1.000	-	-	0.277	0.988
ApproximateEntropy	0.600	1.000	0.534	0.900	0.215	0.992
Random Excursions	0.637	1.000	-	-	0.378	0.990
Rand. Excursions Var.	0.876	1.000	-	-	0.335	0.987
Serial	0.304	0.982	0.740	1.000	0.470	0.992
LinearComplexity	0.868	0.964	0.740	1.000	0.270	0.989

와 발진기 기반의 진 난수 발생기에 대하여 연구를 진행한 논문 4편을 분석하였다. 일반적인 진 난수 발생기는 랜덤소스를 발생시키는 모듈, 랜덤소스를 난수로 샘플링하는 모듈, 그리고 샘플링 된 난수의 질을 높이기 위한 후처리 모듈로 구성이 되며, 그 중에서도 샘플링은 DFF, 후처리는 폰 노이만 방식 [10, 11]을 이용하는 경우가 일반적이다. 그러므로, 랜덤소스의 생성 방법이 진 난수 발생기의 동작과 성능을 결정짓게 되며, 생성된 난수의 질을 높이기 위해 랜덤소스 모듈의 하드웨어 리소스가 굉장히 커지는 경우도 존재한다. 향후 진 난수 발생기 연구는 기존의 발진기나 준안정성을 위해 사용되는 모듈과 동일한 기능을 더 소량의 하드웨어 리소스로 구현하기 위한 방식을 연구 및 개발하는 방향으로 진행할 예정이다.

References

[1] M. Bakiri, C. Guyeux, J.-F. Couchot, and A. K. Oudjida, “Survey on hardware implementation of random number generators on FPGA: Theory and experimental analyses,” *Computer Science Review,* vol.27, pp.135-153, 2018.
DOI: 10.1016/j.cosrev.2018.01.002

[2] I. Vasyltsov, E. Hambardzumyan, Y.-S. Kim, and B. Karpinskyy, “Fast Digital TRNG Based on Metastable Ring Oscillator,” *Berlin, Heidelberg, 2008: Springer Berlin Heidelberg, in Cryptographic Hardware and Embedded Systems,* pp.164-180, *2008.*

[3] M. Majzoobi, F. Koushanfar, and S. Devadas, “FPGA-based true random number generation using circuit metastability with adaptive feedback control,” *in Proc. Cryptograph. Hardw. Embedded Syst. (CHES)*, pp.17-32, 2011.

[4] H. Hata and S. Ichikawa, “FPGA implementation of metastability-based true random number generator,” *IEICE Trans. Inf. Syst.*, vol.E95.D, no.2, pp.426-436, 2012. DOI: 10.1587/transinf.E95.D.426

[5] B. Sunar, W. J. Martin, and D. R. Stinson, “A provably secure true random number generator with built-in tolerance to active attacks,” *IEEE Trans. Comput.,* vol.56, no.1, pp.109-119, 2007. DOI: 10.1109/TC.2007.250627

[6] D. Liu, Z. Liu, L. Li, and X. Zou, “A low-cost low-power ring oscillatorbased truly random number generator for encryption on smart cards,” *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol.63, no.6, pp.608-612, 2016.
DOI: 10.1109/TCSII.2016.2530800

[7] Q. Tang, B. Kim, Y. Lao, K. K. Parhi and C. H. Kim, “True Random Number Generator circuits based on single-and multi-phase beat frequency detection,” *Proceedings of the IEEE 2014 Custom Integrated Circuits Conference,* pp.1-4, 2014. DOI: 10.1109/CICC.2014.6946136

[8] A. P. Johnson, R. S. Chakraborty and D. Mukhopadyay, “An Improved DCM-Based Tunable True Random Number Generator for Xilinx FPGA,” in IEEE Transactions on Circuits and Systems II: Express Briefs, vol.64, no.4, pp.452-456, 2017. DOI: 10.1109/TCSII.2016.2566262

[9] N. Nalla Anandakumar, S. K. Sanadhya and M. S. Hashmi, “FPGA-Based True Random Number Generation Using Programmable Delays in Oscillator-Rings,” *in IEEE Transactions on Circuits and Systems II: Express Briefs,* vol.67, no.3, pp.570-574, 2020. DOI: 10.1109/TCSII.2019.2919891

[10] J. Von Neumann, “Various techniques used in connection with random digits,” *Nat. Bureau Standards Appl. Math. Ser.,* vol.12, pp.36-38, 1951.

[11] V. Rozic, B. Yang, W. Dehaene, and I. Verbauwhede, “Iterating von Neumann’s post-processing under hardware constraints,” *in 2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pp.37-42, 2016. DOI: 10.1109/HST.2016.7495553

[12] L. E. Bassham, III et al., “A statistical test suite for random and pseudorandom number generators for cryptographic applications, Rev. 1a,” U.S. Dept. Commerce, Nat. Inst. Stand. Technol., Rep. SP 800-22, 2010.

BIOGRAPHY

Hwasoo Shin (Member)

2020 : BS degree in Electronics Engineering, Chungnam National University.
2020~: MS degree in Electronics Engineering, Chungnam National University.

Hoyong Yoo (Member)

2010 : BS degree in Electrical & Electronic Engineering, Yonsei University.
2012 : MS degree in Electronics Engineering, KAIST.
2016 : Ph.D. degree in Electronics Engineering, KAIST.
2016 : Researcher, Samsung Electronics.
2016~ : Assistant Professor, Chungnam National University.