난수 발생기의 무작위성 향상을 위한 Discarding 기반 후 처리 회로의 RTL 설계

김재우, 백승범, 잔 타잉 안, 홍종필

충북대학교

kjw@cbungbuk.ac.kr, sbbaek@chungbuk.ac.kr, antt@chungbuk.ac.kr, jphong@chungbuk.ac.kr

A Discarding-based Post-Processing RTL Design for Randomness Improvement of Random Number Generator

Jae-Woo Kim, Seung-Bum Baek, Thanh-An Tran, Jong-Phil Hong

School of Electrical Engineering, Chungbuk National University

요 약

본 논문은 난수 발생기의 무작위성을 향상시켜, NIST(National Institute of Standards and Technology)에서 제공하는 검증 방법인 800-22a[1]의 테스트를 통과하기 위한 Discarding 기반 후처리 기법을 제안한다. 제안하는 회로는 CMOS Samsung-65nm 공정을 활용하여, RTL(Registor Transistor Logic)으로 설계되었다. Discarding 기반 후처리 기법을 적용한 이후 테스트 가능한 난수 발생기의 비트수는 약 40% 감소하였다. 하지만, 15개의 테스트 군 중에서 1×10^8 Bits 이상을 필요로 하는 테스트를 제외한 12개의 테스트 군을 모두 만족하였다.

Ⅰ. 서 론

난수 발생기는 암복호화, 인증, 디지털 서명, 디지털 통신과 같은 다양한 분야에서 중요한 역할을 한다. 특히 보안 시스템에서 비밀 키 생성에 사용되는데, 악의적 공격을 방어할 수 있는 높은 무작위성을 갖는 난수 생성을 필요로 한다. 본 논문에서는 기존의 난수 발생기에 적용할 수 있는 무작위성 향상을 위한 Discarding 기반 후처리 회로를 제안한다. 제안하는 회로는 기존의 Ring Oscillator TRNG(True Random Number Generator) 회로에 결합하여 NIST에서 제공하는 무작위성 검증 도구인 SP 800-22a의 테스트를 통하여 난수 발생기에서 생성된 출력의 성능을 검증하고자 한다.

Ⅱ. 본 론

무작위한 비트열이란 0과 1이라는 숫자가 양면에 적힌 동전을 던졌을 때 나오는 결과와 같다. 이때 앞면과 뒷면이 나타날 확률은 각각 1/2이며 독립적이다. 독립적으로 만들어진 비트로 구성된 비트열은 다음 비트열을 예측할 수 없다.

양방향 통신 기능을 갖춘 소형 장치들의 활용성이 증가함에 따라 정보보안 인증 과정에서 하드웨어의 암호화를 필요로 한다. 이때, 난수 발생기는 하드웨어 조건에 맞는 암호화에 필요한 비밀키를 생성하게 되며 외부의 악의적 공격을 방어할 수 있을 만큼의 높은 무작위성을 갖는 난수 발생기를 필요로 한다.

연구에 사용된 난수 발생기는 32-bit Ring Oscillaotr TRNG[2]이며 TRNG는 PRNG(Pseudo Random Number Generator)와 다르게 비결정론적 엔트로피를 사용한다. 하지만, CMOS TRNG의 출력은 보안 분야에서 사용하기에 충분한 무작위성을 확보하지 못한다는 문제점이 있고, 따라서 이를 극복하기 위해 von Neumann corrector, XOR corrector, Code corrector와 같은 다양한 후처리 회로가 수차례 연구되었다. [4] 하지만, TRNG의 출력을 PRNG의 입력으로 사용하는 방법들은 문제를 근본적으로 해결하지 못하며, 면적 및 전력 소비가 크다는 단점이 존재한다. 본 논문에서는 TRNG의 무작위성을 확보하기 위해서 다음과 같은 Discarding Method를 제안한다. 그림 1과 같이 TRNG의 연속적인 출력을 비교 가능할 만큼 충분히 저장한다(32 bits×10번 반복). 이후, 저장된 값을 모두 더하여 threshold value와 비교한다. Threshold value를 선정하기 위해 0이 아닌 모든 수의 합을 의미하는 Hamming Weight [5]을 사용하였다. 이상적인 TRNG의 320 bits 평균 Hamming Weight은 160이며 TRNG의 반복 측정으로 저장된 값의

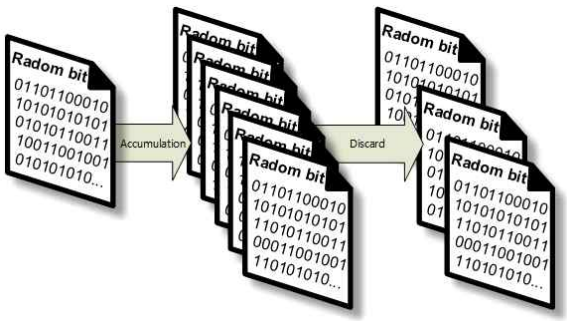

그림 1. Discarding Method의 간략한 소개

Hamming Weight이 $160+\gamma$를 초과하거나 $160-\gamma$미만일 경우에는 Discard 하게 된다. NIST 800-22a 문서의 특정 테스트에서 요구하는 테스트 당 최소 테스트 Bits는 1×10^6 Bits이며, 최소의 α(level of significance)값인 0.01을 선택할 경우 각 테스트 당 총 100번의 테스트가 진행되기 때문에 필요한 총 Bits는 1×10^8 Bits이다. 그림 2에서는 γ의 값에 따른 Shannon Entropy와 테스트 가능한 Bit의 수를 보여주고 있다. 테스트에 사용된 γ의 값은 8이며 총 비트의 수는 7×10^7 Bits로 Discarding Method를 반복 적용한 이후 2.4×10^7 Bits가 Discard 되어 4.6×10^7 Bits가 최종 테스트에 사용되었다. 생성된 난수 발생기의 성능을 검증하기 위해 NIST 800-22a의 검증 방법을 활용하였다. 문서는 총 15개의 테스트로 구성되어 있으며 각 테스트는 가설 검정을 기반으로 한다. 영 가설(null hypothesis)기법을 채택하면

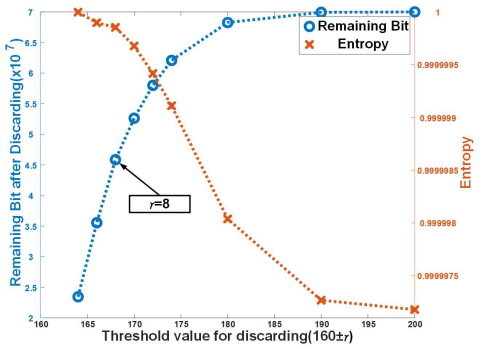

그림 2. Shannon Entropy와 테스트 가능한 Bits 사이의 Trade-off 관계

"난수 발생기가 생성한 비트열이 랜덤하다."라는 가정하에 테스트가 진행된다. 이 가설이 기각될 경우에 나타나는 에러를 Type 1 에러라고 하며, 이를α(level of significance)라고 한다. 반대로 대립가설(alternative hypothesis)은 "난수 발생기가 생성한 비트열이 랜덤하지 않다"라는 가정이다. 이 가설이 기각될 경우 나타나는 에러를 Type 2 에러라고 하며, 이를 β라고 한다. α의 경우에는 사용자가 [0.001, 0.01]범위에서 선택 가능하며 암호학에서 α의 값은 약 0.01이다. α값을 0.01로 선택한 본 논문에서는 테스트당 최소 100번의 테스트가 진행된다. 각 테스트는 P-value ≥ 0.0001, Proportion $\geq 96/100$ 을 만족하여야 한다. 이때 1번의 테스트 당 1×10^6 Bits을 필요로 하는 하위 3개의 테스트(Overlapping Test, Random Excursions Test, Random Excursions Variant Test)는 테스트 불가능하다. 결과적으로, 제안하는 Discarding Method를 적용한 결과 12개의 테스트 군을 모두 만족하였다.

표 1. Discarding Method 적용 전 NIST TEST 결과

Test	P-value	Proportion
Frequency	0.000000	94/100
Frequency within a Block	0.337692	96/100
Runs Test	0.599313	96/100
Cumulative Sums	0.000000	93/100
Longest Run	0.019951	99/100
Rank	0.639667	96/100
FFT	0.256891	98/100
Non-overlapping	FAIL(sub-test 148)	
Overlapping	-	-
Universal	0.351900	96/100
Random Excursions	-	-
Random Excursions Variant	-	-
Approximate Entropy	0.329154	96/100
Serial	0.315716	96/100
Linear	0.254129	94/100

표 2. Discarding Method 적용 후 NIST TEST 결과

Test	P-value	Proportion
Frequency	0.911413	98/100
Frequency within a Block	0.867692	99/100
Runs Test	0.699313	98/100
Cumulative Sums	0.595549	96/100
Longest Run	0.759756	99/100
Rank	0.289667	99/100
FFT	0.494392	100/100
Non-overlapping	PASS(sub-test 148)	
Overlapping	-	-
Universal	0.275700	96/100
Random Excursions	-	-
Random Excursions Variant	-	-
Approximate Entropy	0.457516	98/100
Serial	0.935716	99/100
Linear	0.554420	98/100

Ⅲ. 결 론

본 논문에서는 기존의 CMOS TRNG는 보안 분야에 사용하기에 충분한 무작위성을 확보하지 못한다는 단점을 보완하고자 Discarding 기반의 후처리 기법을 제안한다. 연속적으로 출력된 데이터를 비교 가능할 만큼 충분히 저장한다. 이후, threshold value와 비교하여 조건을 만족하지 못할 경우 데이터를 Discard 하게 된다. 난수 발생기 출력의 성능을 검증하기 위한 방법으로는 NIST 800-22a의 문서에서 제공되는 테스트를 활용하였다. 회로는 RTL로 설계되었으며 15개의 테스트 중에서 1×10^8 Bits이상을 필요로 하는 3개의 테스트를 제외한 12개의 테스트를 모두 만족 하였다.

ACKNOWLEDGMENT

이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2021R1A2C2005258). 본 연구는 과학기술정보통신부 및 정보통신기획평가원의 지역지능화혁신인재양성(Grand ICT연구센터) 사업의 연구결과로 수행되었음(IITP-2021-2020-0-01462).

참 고 문 헌

[1] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M.Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", NIST Special Publication 800-22,,2001.

[2] K. Wold and S. Petrović, "Behavioral Model of TRNG Based on OscillatorRings Implemented in FPGA," in Proc. IEEE Int. Symp. Design DiagnosticElectron. Circuits Syst., Apr. 2011, pp. 163 - 166.

[3] Yang, Kaiyuan, et al. "16.3 A 23Mb/s 23pJ/b fully synthesized true-random-number generator in 28nm and 65nm CMOS." 2014 IEEE International Solid-State Circuits Conference Digest of Technical Papers (ISSCC). IEEE, 2014.

[4] S. V. Suresh and W. P. Burleson, "Entropy and energy bounds for metastability based TRNG with lightweight post-processing," IEEE Trans.Circuits Syst. I, Reg. Papers, vol. 62, no. 7, pp. 1785 - 1793, Jul. 2015.

[5] R. Maes, and I. Verbauwhede, "Physically Unclonable Functions: a Study on the State of the Art and Future Research Directions," *Towards Hardware-Intrinsic Security*, Springer, Oct. 2010.