ISSN : 1226-7244 (Print)
ISSN : 2288-243X (Online)
논문번호 20-01-08
52
j.inst.Korean.electr.electron.eng.Vol.24,No.1,52~58,March 2020
http://dx.doi.org/10.7471/ikeee.2020.24.1.52

무작위 천이규칙을 갖는 셀룰러 오토마타 기반 참난수 발생기

True Random Number Generator based on Cellular Automata with Random Transition Rules

최 준 백*, 신 경 욱*★

Jun-Beak Choi*, Kyung-Wook Shin*★

Abstract

This paper describes a hardware implementation of a true random number generator (TRNG) for information security applications. A new approach for TRNG design was proposed by adopting random transition rules in cellular automata and applying different transition rules at every time step. The TRNG circuit was implemented on Spartan-6 FPGA device, and its hardware operation generating random data with 100 MHz clock frequency was verified. For the random data of 2×10^7 bits extracted from the TRNG circuit implemented in FPGA device, the randomness characteristics of the generated random data was evaluated by the NIST SP 800-22 test suite, and all of the fifteen test items were found to meet the criteria. The TRNG in this paper was implemented with 139 slices of Spartan-6 FPGA device, and it offers 600 Mbps of the true random number generation with 100 MHz clock frequency.

요 약

정보보안 응용을 위한 참난수 발생기(true random number generator; TRNG)의 하드웨어적 구현에 대하여 기술한다. 셀룰러 오토마타에 무작위 천이규칙을 도입하고, 매 시간단계마다 다른 천이규칙이 적용되는 새로운 방법을 제안하였다. 설계된 참난수 발생기를 Spartan-6 FPGA 소자에 구현하고, 100 MHz 동작 주파수에서 난수 생성동작을 검증하였다. FPGA 소자에 구현된 참난수 발생기로부터 2×10^7 비트의 난수 데이터를 추출하여 NIST SP 800-22 테스트를 통해 생성된 난수 데이터의 무작위 성능을 검증하였으며, 15개의 테스트 항목 모두 기준을 충족하는 것으로 확인되었다. 본 논문의 참난수 발생기는 Spartan-6 FPGA 소자의 139 슬라이스로 구현되었고, 100 MHz 동작 주파수에서 600 Mbps의 참난수 생성 성능을 갖는다.

Key words : TRNG, Random Number Generation, Cellular Automata, Transition Rule, Information Security

---

* School of Electronic Engineering, Kumoh National Institute of Technology
★ Corresponding author
E-mail : kwshin@kumoh.ac.kr, Tel : +82-54-478-7427

※ Acknowledgment
- This research was supported by the KIAT (Korea Institute for Advancement of Technology) grant funded by the Korea Government (MOTIE : Ministry of Trade Industry and Energy). (No. N0001883, HRD Program for Intelligent semiconductor Industry)
- This work was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (No. 2017R1D1A3B03031677)
- Authors are thankful to IDEC for supporting EDA software.

Manuscript received Feb. 14, 2020; revised Mar. 19, 2020; accepted Mar. 24, 2020.

Ⅰ. 서론

난수(random number)는 정보보안 시스템을 비롯하여 Monte Carlo 시뮬레이션, 반도체 테스트, 통계분석, 도박, 복권 등 매우 다양한 분야에서 중요하게 사용된다. 정보보안 시스템에서는 대칭키 암호를 위한 비밀키 생성, 공개키 암호 시스템의 개인키와 공개키 생성, 전자서명 시스템 등에 난수가 필수적으로 사용되며, 암호 시스템의 안전성은 사용되는 난수의 예측 불가능성에 의해 좌우된다[1].

난수를 생성하는 난수 발생기는 크게 나누어 의사난수 발생기(pseudo-random number generator; PRNG)와 참난수 발생기(TRNG)로 분류된다. 의사난수 발생기는 결정론적 시스템을 이용하는데, 결정론적 시스템은 일정한 알고리듬을 따라 입력에 의해 출력이 결정된다. 의사난수는 일정 주기로 데이터가 반복되는 형태를 갖지만, 그 주기가 매우 큰 경우에는 난수로 간주할 수 있다. 그러나 알고리듬과 초기 값을 알고 있다면 결과를 유추할 수 있는 단점을 갖는다. 의사난수 생성방법으로 선형 합동 생성기(linear congruential generator), 선형 피드백 시프트 레지스터(linear feedback shift register; LFSR), B.B.S(Blum Blum Shub), 셀룰러 오토마타(cellular automata; CA) 등이 제안되고 있다[2].

참난수 발생기는 동일한 환경에서 동일한 초기 값을 이용하더라도 출력 값을 예상할 수 없는 것이 특징이다. 참난수 발생기는 알고리듬을 이용해 난수를 생성하는 의사난수 발생기와 달리 불규칙적인 자연현상을 숫자로 변환해 난수를 생성한다. 컴퓨터 기술이 발달하면서 의사난수 발생기 패턴의 노출이 가능해졌고, 이를 해결하기 위한 방법으로 참난수 발생기가 널리 사용되고 있다. 참난수 발생기의 하드웨어 설계를 위해 자연계에 존재하는 다양한 형태의 잡음, 링 발진기(ring oscillator; RO) 구조, 준안정 상태(metastability), 양자역학적 현상의 이용 등 다양한 방법들이 제안되고 있다[3].

본 논문에서는 의사난수 발생기의 한 방법인 셀룰러 오토마타를 이용하여 참난수 발생기를 설계하였다. 셀룰러 오토마타에 잡음과 무작위 천이규칙을 도입하여 참난수 데이터를 생성하는 방법을 제안한다. Ⅱ장에서는 셀룰러 오토마타의 개념, 동작방법과 형태, 하드웨어 설계의 선행 연구에 대해 소개하고, Ⅲ장에서는 무작위 천이규칙을 적용한 셀룰러 오토마타 기반의 TRNG 하드웨어 설계에 대해 설명한다. Ⅳ장에서는 설계된 참난수 발생기의 무작위 특성 평가결과에 대해 기술하고, Ⅴ장에서 결론과 향후 연구방향에 대해 기술한다.

Ⅱ. 셀룰러 오토마타

1. 셀룰러 오토마타[4]

CA는 수학, 물리학, 생물학 등 다양한 분야에서 이산 동적 시스템으로 사용되는 결정론적 시스템 중 하나이다. CA는 Z, Q, V, f의 4가지 요소로 정의할 수 있다. Z는 d 차원의 셀 공간을 나타내는 지표로, d=1인 경우 셀들이 1열로 배열되고, d=2는 평면 형태이다. Q는 셀이 가질 수 있는 상태로 구성된 집합을 나타내고, f는 현재 상태가 결정되는 천이규칙(transition rule)이며, V는 천이규칙 f에서 사용되는 인접한 이웃 셀을 나타낸다[4]. CA는 셀의 배열로 구성되며, 각각의 셀의 현재 상태는 이전 상태의 인근 셀들의 데이터와 주어진 천이규칙에 따라 결정된다. CA는 결정론적 시스템이므로 4가지 요소 Z, Q, V, f와 초기 값이 정해지면 시간단계 별 결과를 유추할 수 있다.

CA의 동작은 식 (1)과 같이 표현되며, 규칙에 사용된 인근 셀의 집합은 $\{x,x_1,\dots,x_N\}\in V$ 이고, $a_i(n)$는 i-번째 셀의 시간단계 n에서의 상태를 나타낸다.

$$a_i(n+1)=f\left(a_{i+x_0}(n),a_{i+x_1}(n),\dots,a_{i+x_N}(n)\right) \quad (1)$$

Elementary cellular automata(ECA) [5]는 CA의 가장 단순한 모델 중 하나로, 그 동작은 식 (2)와 같이 표현된다. ECA는 1 차원적 셀 공간을 가지고(Z), 각 셀은 0, 1의 2가지 상태를 가질 수 있다($\{0,1\}\in Q$). 또한 셀은 이전 시간단계의 자신과 바로 인접한 두 셀의 영향만을 받는다($\{-1,0,1\}\in V$).

$$a_i(n+1)=f\left(a_{i-1}(n),a_i(n),a_{i+1}(n)\right) \quad (2)$$

그림 1은 ECA의 천이규칙 표현 방법을 보인 예이며, 현재 시간단계에서 가능한 모든 이웃 셀들의 상태를 나열하고, 다음 시간단계의 각각의 셀 상태를 이용하여 다음 시간단계에서 얻어지는 이진 값들의 십진수 대응 값으로 나타낸다.

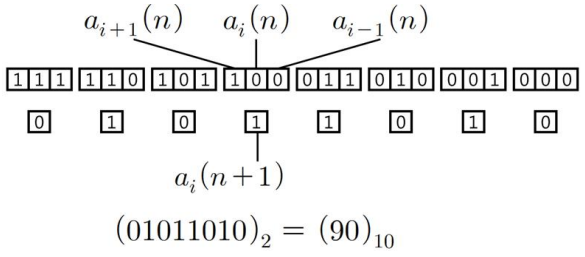

Fig. 1. Representation of ECA transition rule in Wolfram notation (in the case of R-90) [10].
그림 1. Wolfram 표기법에 의한 ECA 천이규칙 표기 (R-90의 경우) [10]

2. 메모리를 갖는 셀룰러 오토마타

Cellular automata with memory(CAM)는 1990년 Edward Fredkin에 의해 제안된 CA의 한 형태로 메모리가 추가된 구조이다[6]. CAM 셀의 다음 상태는 셀의 현재 상태뿐만 아니라 메모리에 저장된 이전 상태의 값에도 영향을 받는다. Fredkin의 CAM 동작은 식 (3)과 같이 표현되고, 이전 시간단계 $(n-1)$의 상태가 다음 시간단계 $(n+1)$의 상태에 영향을 미친다.

$$a_i(n+1) = f(a_{i-1}(n), a_i(n), a_{i+1}(n), a_i(n-1)) \quad (3)$$

식 (3)의 CAM은 직전 시간단계와 현재 시간단계의 상태만 기억하고 사용할 수 있는 메모리 공간을 필요로 한다. 기본 CAM 외에 다양한 형태의 CAM들이 제안되었다[7, 8].

2017년 E. Göncü Emre와 M.E. Yalçın에 의해 랜덤 메모리를 갖는 CA(CARM)이 제안되었으며[9-11], 현재의 셀 상태와 과거의 셀 상태 중 무작위로 선택하여 사용하도록 설계되었다. 그림 2는 CARM 중 하나인 elementary cellular automata with random minimal memory(ECARMM)의 배열 및 연결 방법을 보인 것이며, ECARMM의 동작은 식 (4)와 같이 표현된다.

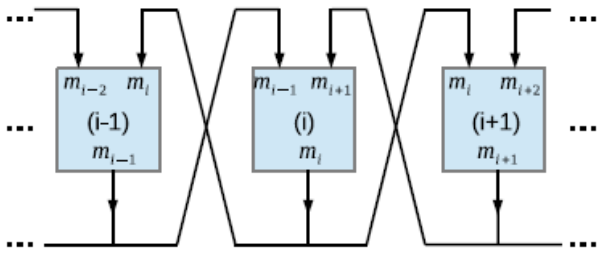

Fig. 2. Connection scheme between cells of ECARMM [10].
그림 2. ECARMM의 셀들 간 연결 구조 [10]

$$a_i(n+1) = f(a_{i-1}(n-\tau_{i-1}(n)), a_i(n-\tau_i(n)), a_{i+1}(n-\tau_{n+1}(n))) \quad (4)$$

III. 무작위 천이규칙을 갖는 CA 기반 참난수 발생기 설계

본 논문에서는 셀룰러 오토마타에 잡음과 무작위 천이규칙을 도입한 참난수 발생기(CA with Random Rule; CARR-TRNG) 구조를 제안한다. 제안되는 CARR-TRNG는 그림 3의 구조를 가지며, 내부에 지연라인(delay line)을 갖는 Dcell의 배열, 지연라인을 갖지 않는 Ncell의 배열, 천이규칙을 저장하는 룰박스(rule box)로 구성된다. CARR은 ECA의 변형으로 1차원적 셀 공간과 $\{-1,0,1\}\in V$, $\{0,1\}\in Q$의 요소 값을 갖는다. CARR의 동작은 지연을 갖지 않는 일반 셀(Ncell)의 식 (2)와 지연라인을 갖는 셀(Dcell)의 식 (4)로 나타낼 수 있고, 일반 셀과 지연라인을 갖는 셀 모두 출력 데이터 생성에 사용된다.

본 논문에서 제안하는 CARR-TRNG는 지연라인의 지터잡음을 이용한 무작위성을 엔트로피 소스로 사용한다. Dcell 내부의 지연라인을 통해 플립플롭의 준비시간, 유지시간이 위반되도록 하여 현재의 상태나 직전의 상태 중 하나가 무작위로 선택되도록 한다. 지연라인의 크리티컬 패스(critical path) 지연이 근사적으로 클록주기와 같아지도록 설정하면 플립플롭의 출력이 불확정성을 갖게 되므로, 무작위성의 엔트로피 소스로 사용될 수 있다.

지연라인을 갖는 Dcell의 내부 구성은 그림 4와 같으며, 셀의 상태 데이터를 저장하는 플립플롭, 무작위성을 부여하기 위한 지연라인 및 무작위성극대화를 위한 XOR 게이트, 그리고 다음 시간단계의 플립플롭 상태 값을 결정하는 Comb_Logic으로 구성된다. Dcell은 플립플롭에 저장되는 초기 값 Init_val

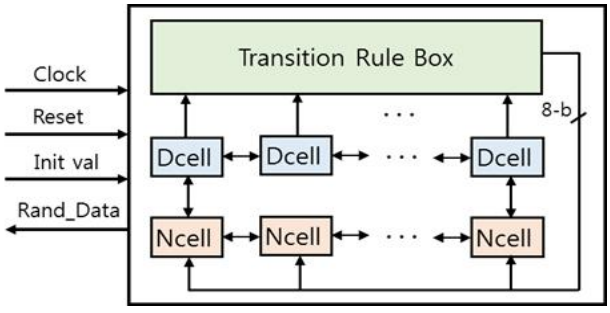

Fig. 3. Block diagram of CARR-TRNG.
그림 3. CARR-TRNG의 내부 블록도

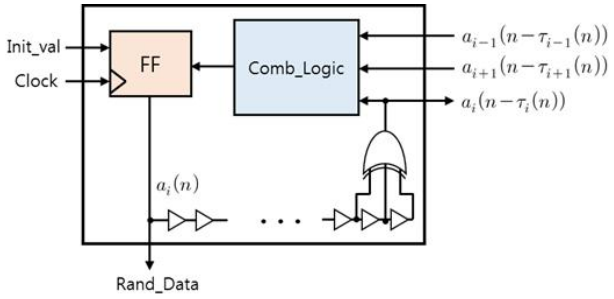

Fig. 4. Block diagram of Dcell with delay line.
그림 4. 지연라인을 갖는 Dcell의 내부 블록도

와 자신의 좌·우 셀의 상태 값을 입력받는다. Dcell은 자신의 좌·우 셀들과 그림 2의 형태로 연결되며, 좌·우 셀들로부터 입력되는 상태 값 $a_{i-1}(n-\tau_{i-1}(n))$, $a_{i+1}(n-\tau_{i+1}(n))$과 자신의 상태 값 $a_i(n-\tau_i(n))$을 이용하여 다음 상태 값을 결정한다. 이때 자신의 상태 값 $a_i(n)$이 지연라인을 거쳐 지터잡음을 갖는 데이터 $a_i(n-\tau_i(n))$가 되고, Comb_Logic으로 입력된다. Dcell의 Comb_Logic은 미리 정의된 천이규칙에 따라 출력 값을 결정한다. 이때 지연라인에 의해 크리티컬 패스 지연이 클록주기와 유사하게 설정되고, 이에 의해 플립플롭의 준비시간, 유지시간을 위반하여 플립플롭에 저장되는 상태 값이 무작위성을 갖게 된다.

한편, 지연라인을 구성하는 지연소자 개수가 고정되면 특정 반도체 제조공정 또는 FPGA 디바이스에 구현되었을 때 지연 값이 고정되어 클록주기와 유사한 지연의 발생이 보장되지 않을 수 있으며, 또한 FPGA 디바이스에 따라 지연라인의 지연 값이 달라 플립플롭의 준비시간, 유지시간 위반이 발생하지 않으며, 따라서 무작위성이 얻어지지 않을 수 있다. 이러한 문제점을 보완하고자 본 논문에서는 그림 4에서 보는 바와 같이 지연라인에 XOR 게이트를 추가하였다. 지연라인에서 클록주기와 유사한 지연을 갖는 부분에 XOR 게이트를 추가하여 Comb_Logic에 입력되는 데이터 $a_i(n-\tau_i(n))$가 빠른 진동을 갖도록 하였다. 이를 통해 Comb_Logic의 출력이 플립플롭에 입력될 때 빠른 진동이 일어나 무작위성을 극대화할 수 있으며, 지연라인의 지연 값이 고정되어 생기는 문제점을 해결하였다.

룰박스는 Dcell의 상태 데이터를 입력으로 받아 (그림 3 참조) 미리 정의된 천이규칙들 중 하나를 출력하며, 출력된 천이규칙은 Ncell의 입력으로 사

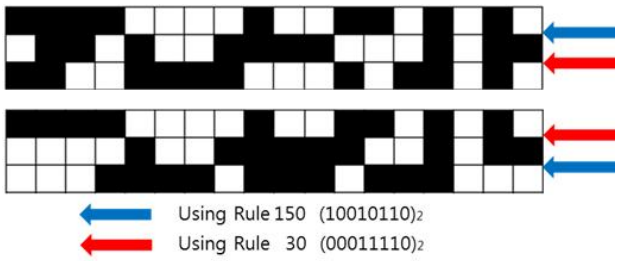

Fig. 5. Results obtained from different transition rules (black and white denote '1' and '0', respectively).
그림 5. 서로 다른 천이규칙에 의한 결과 (흑색과 백색은 각각 '1'과 '0'을 나타냄)

용된다. 본 설계에서는 룰박스에 정의되는 천이규칙을 Rule-30, Rule-45, Rule-90, Rule-150의 네 가지로 정의하였으며, 룰박스에 정의되는 천이규칙은 설계자가 임의로 결정할 수 있다. 룰박스는 룩-업 테이블(look-up table) 형태로 구현되었으며, 입력되는 Dcell의 상태 데이터가 룩-업 테이블의 주소 값으로 사용되어 저장된 천이규칙 중 하나가 출력된다.

이때 룰박스로 입력되는 Dcell의 상태 데이터는 무작위성을 갖고 있으므로, 룰박스에서 선택되는 천이규칙 또한 무작위성을 갖는다. 무작위성을 갖는 천이규칙은 Ncell로 입력되어 Ncell의 데이터를 예측 불가능하게 만든다. 예를 들어, 그림 5는 동일한 초기 값에서 시작하더라도 서로 다른 천이규칙이 적용되거나 천이규칙의 순서가 다르게 적용되면 전혀 다른 결과 값이 출력됨을 보이고 있다. 이와 같은 방법으로 무작위 천이규칙을 Ncell에 적용하여 Ncell의 상태 값에 무작위성을 부여할 수 있다.

그림 6은 지연을 갖지 않는 Ncell의 내부 블록도이며, 셀의 상태 값을 저장하는 플립플롭, 좌·우 셀의 상태 값과 자신의 상태 값에 따라 다음 시간 단계의 상태 값을 결정하는 Comb_Logic으로 구성된다. Ncell은 플립플롭의 초기 값, 좌·우 셀의 상태 값 그리고 룰박스로부터 천이규칙을 입력 받는

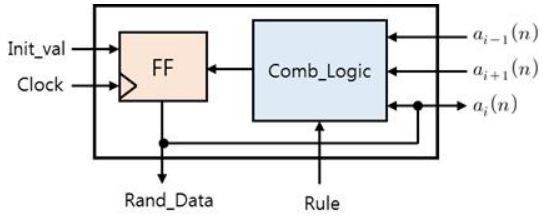

Fig. 6. Block diagram of Ncell without delay line.
그림 6. 지연라인이 없는 Ncell 셀의 내부 블록도

다. Ncell의 Comb_Logic은 Dcell의 Comb_Logic과 다르게 천이규칙이 미리 정의되어 있지 않으며, 룰 박스로부터 입력되는 천이규칙을 기반으로 $a_i(n)$, $a_{i+1}(n)$, $a_{i-1}(n)$ 데이터를 이용하여 출력 값을 결정한다. Ncell은 내부에 지연라인과 XOR 게이트가 없어 자체적으로는 무작위 데이터를 생성하지 못한다. 그러나 입력되는 무작위 천이규칙에 따라 각 시간단계마다 Comb_Logic의 천이규칙이 다르게 적용되므로, 셀의 현재 상태 값이 동일하더라도 플립플롭에 저장되는 다음 상태 값이 무작위성을 갖게 된다.

Ⅳ. FPGA 구현 및 무작위 특성 평가

본 논문에서 제안하는 CARR 기반 TRNG의 하드웨어 동작을 확인하기 위해 7개의 Dcell과 53개의 Ncell (총 60개 셀)로 구성되는 CARR-TRNG 회로를 설계하였다. FPGA 디바이스에 구현된 CARR-TRNG의 목표 동작 주파수를 100 MHz로 설정하였으며, 시뮬레이션을 통해 지연라인의 지연이 근사적으로 10 ns가 되도록 설계하였다. 설계된 CARR-TRNG 회로를 Spartan-6 FPGA 디바이스에 구현하여 출력되는 데이터의 무작위 특성을 평가하였다. CARR은 CA의 한 형태이므로, 각 시간단계의 상태 데이터는 이전 시간단계에서의 이웃 셀 상태 데이터와 연관성을 갖는다. 이웃 셀 간의 연관성을 줄이기 위해 설계된 CARR-TRNG를 구성하는 60개의 셀 중 6개(10, 20, 30, 40, 50, 60번째)의 셀 데이터만을 출력하여 총 2×10^7 비트의 데이터로 무작위 특성을 평가하였다. 무작위 특성 평가는 NIST 800-22 테스트[12]를 적용하였으며, 그 결과는 표 1과 같다. 15개의 평가항목 모두 기준을 만족하였으며, 이를 통해 Spartan-6 FPGA 디바이스에 구현되어 100 MHz 주파수로 동작하는 CARR-TRNG가 참난수 생성기로 동작함을 확인하였다.

그림 7은 FPGA에 구현된 60개의 셀을 갖는 CARR-TRNG에 초기 값 “000 0000 2000 0000”를 넣고, 100 시간단계 동안의 각 셀의 상태를 나타낸 것이다. 그림 7의 실험결과로부터, 동일한 조건에서 동일한 초기 값으로 동작하더라도 서로 다른 무작위 데이터가 생성되어 CARR-TRNG가 참난수 발생기로 동작함을 확인할 수 있다.

CARR-TRNG는 Spartan-6 FPGA 디바이스로 합성한 결과 139 슬라이스로 구현되었으며, 100 MHz의 동작 주파수에서 600 Mbps의 난수 생성 성능을 갖는다. 표 2는 문헌에 발표된 참난수 발생기와 본 논문의 CARR 기반 참난수 발생기의 성능을 비교한 것이다. 본 논문의 CARR-TRNG는 문헌에 발표된 참난수 발생기보다 난수 생성 성능이 우수하며, 면적 대비 처리량 또한 뛰어남을 알 수 있다. 제안된 CARR-TRNG는 CA를 구성하는 셀 개수의 변경을 통해 초당 생성되는 랜덤 데이터를 원하는 대로 조절할 수 있다는 장점을 갖는다.

Table 1. Results of randomness test using NIST 800-22.
표 1. NIST 800-22에 의한 무작위 특성 테스트 결과

Statistical Test	P-value	Success Proportion	Result
Frequency	0.739918	1	Pass
Block Frequency	0.534146	1	Pass
Cumulative	0.066882 0.637119	1	Pass
Runs	0.739918	1	Pass
Longest Run	0.437274	1	Pass
Rank	0.739918	1	Pass
FFT	0.534146	1	Pass
Non Overlapping Template	-	0.97959	Pass
Overlapping Template	0.911413	1	Pass
Universal	0.162606	0.95	Pass
Approximate Entropy	0.162606	1	Pass
Random Excursions	-	1	Pass
Random Excursions Variant	-	1	Pass
Serial	0.637119	0.95	Pass
Linear Complexity	0.035174	1	Pass

(a) run-1 (b) run-2

Fig. 7. True random data generation results of CARR-TRNG operated with the same initial value (black and white denote ‘1’ and ‘0’, respectively).
그림 7. 동일한 초기값으로 동작한 CARR-TRNG의 참난수 데이터 생성 결과 (흑색과 백색은 각각 ‘1’과 ‘0’을 나타냄)

Table 2. Comparison of TRNGs.
표 2. TRNG 비교

Ref. No	Entropy Source	FPGA device	Area [slices]	Throughput [Mbps]	Throughput/Area [Mbps/slice]
[13]	RO	Spartan-6	67	14.3	0.213
[14]	PLL	Kintex-7	19	6.25	0.329
[15]	RO	Spartan-6	60	130	2.167
[16]	RO	Virtex-6	25	100	4.0
[17]	RO	Spartan-3	528	6	0.011
[18]	D-Latch	Virtex-6	224	50	0.223
This Paper	CA	Spartan-6	139	600	4.316

Ⅴ. 결론

본 논문에서는 무작위 천이규칙을 적용한 셀룰러 오토마타 기반의 참난수 발생기를 제안하였으며, 제안된 CARR-TRNG를 Spartan-6 FPGA 디바이스에 구현하여 100 MHz의 동작 주파수에서 참난수 발생기로 동작함을 확인하였다. 제안된 CARR-TRNG는 셀의 개수를 증가시켜 한 클록 주기에 생성되는 무작위 난수의 양을 늘릴 수 있는 장점이 있다. 또한, 기존의 CARM과 달리 모든 셀에 지연라인이 존재하지 않기 때문에 셀의 개수 증가에 따른 면적 효율성을 갖는다. 본 논문의 CARR-TRNG에서는 지연라인에 의한 지연이 클록주기에 근접하도록 설계하는 방법을 적용하였으나, 지연라인 대신 엔트로피 소스를 얻는 다른 방법을 적용하여 CARR 기반의 TRNG를 설계하는 것도 가능하다.

References

[1] M. Grujić, V. Rožić, B. Yang and I. Verbauwhede, “A Closer Look at the Delay-Chain based TRNG,” *2018 IEEE International Symposium on Circuits and Systems (ISCAS)*, Florence, pp.1-5, 2018. DOI: 10.1109/ISCAS.2018.8351222

[2] F. James, “A review of pseudorandom number generators,” *Computer Physics Communications*, Vol.60, No.3, pp.329-344, 1990. DOI: 10.1016/0010-4655(90)90032-V

[3] S. Callegari, R. Rovatti and G. Setti, “Embeddable ADC-based true random number generator for cryptographic applications exploiting nonlinear signal processing and chaos,” *IEEE Transactions on Signal Processing*, vol.53, no.2, pp.793-805, 2005. DOI: 10.1109/TSP.2004.839924

[4] J. Von Neumann and A. W. Burks, “Theory of self-reproducing automata,” *IEEE Transactions on Neural Networks*, Vol.5, No.1, pp.3-14, 1966.

[5] S. Wolfram, “Statistical mechanics of cellular automata,” *Reviews of Modern Physics*, Vol.55, No.3, pp.601-644, 1983.

[6] T. Toffoli and N. H. Margolus, “Invertible cellular automata: a review,” *Physica D: Nonlinear Phenomena,* vol.45, pp.229-253, 1990.

[7] E. Göncü and M.E. Yalçın, “A new Cellular Automata model with Memory and its FPGA implementation,” *2014 14th International Workshop on Cellular Nanoscale Networks and their Applications (CNNA)*, pp.1-2, 2014. DOI: 10.1109/CNNA.2014.6888627

[8] R. Alonso-Sanz and M. Martín, “One-dimensional cellular automata with memory in cells of the most frequent recent value,” *Complex Systems*, Vol.15, No.3, pp.203-236, 2005.

[9] E. Goncu and M. Yalcin, “Cellular automata with random memory and its implementations,” *International Journal of Bifurcation and Chaos*, Vol. 27, No.5, pp.1-15, 2017. DOI: 10.1142/S0218127417300178

[10] E. Göncü, A. Koçdoğan and M. E. Yalçin, “A High Speed True Random Number Generator with Cellular Automata with Random Memory,” *2018 IEEE International Symposium on Circuits and Systems (ISCAS)*, Florence, pp.1-5, 2018. DOI: 10.1142/S0218127417300178

[11] E. Göncü and M. E. Yalçın, “Realization of elementary cellular automata with random minimal memory,” *2017 European Conference on Circuit Theory and Design (ECCTD)*, Catania, pp.1-4, 2017. DOI: 10.1142/S0218127417300178

[12] Special Publication (NIST SP)-800-22 Rev 1a, A Statistical Test Suite for Random and Pseudo-random Number Generators for Cryptographic Applications, 2010.

[13] V. Rozic, B. Yang, W. Dehaene and I. Verbauwhede, “Highly efficient entropy extraction for true random number generators on FPGAs,” *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, San Francisco, pp.1-6, 2015. DOI: 10.1145/2744769.2744852

[14] N. Deák, T. Györfi, K. Márton, L. Vacariu and O. Cret, “Highly Efficient True Random Number Generator in FPGA Devices Using Phase-Locked Loops,” *2015 20th International Conference on Control Systems and Computer Science*, Bucharest, pp.453-458, 2015. DOI: 10.1109/CSCS.2015.19

[15] B. Yang, V. Rožić, N. Mentens and I. Verbauwhede, “On-the-fly tests for non-ideal true random number generators,” *2015 IEEE International Symposium on Circuits and Systems (ISCAS)*, Lisbon, pp.2017-2020, 2015. DOI: 10.1109/iscas.2015.7169072

[16] G. Ma, H. Liang, L. Yao, Z. Huang, M. Yi, X. Xu and K. Zhou, “A Low-Cost High-Efficiency True Random Number Generator on FPGAs,” *2018 IEEE 27th Asian Test Symposium (ATS)*, Hefei, pp.54-58, 2018. DOI: 10.1109/ATS.2018.00021

[17] N. N. Anandakumar, S. K. Sanadhya and M. S. Hashmi, “FPGA-Based True Random Number Generation Using Programmable Delays in Oscillator-Rings,” *IEEE Transactions on Circuits and Systems II: Express Briefs,* 2019. DOI: 10.1109/TCSII.2019.2919891

[18] X. Yang and R. C. C. Cheung, “A complementary architecture for high-speed true random number generator,” *2014 International Conference on Field-Programmable Technology (FPT)*, Shanghai, pp.248-251, 2014. DOI: 10.1109/FPT.2014.7082786

BIOGRAPHY

Jun-Baek Choi (Member)

2019 : BS degree in Electronic Engineering, medical IT convergence engineering, Kumoh National Institute of Technology.
2019~ : Graduate student, Kumoh National Institute of Technology

Kyung-Wook Shin (Member)

1984 : BS degree in Electronic Engineering, Korea Aerospace University
1986 : MS degree in Electronic Engineering, Yonsei University
1990 : Ph.D. degree in Electronic Engineering, Yonsei University
1990~1991 : Senior Researcher, Semiconductor Research Center, Electronics and Telecommunications Research Institute (ETRI)
1991~ : Professor in School of Electronic Engineering, Kumoh National Institute of Technology
1995~1996 : University of Illinois at Urbana-Champaign (Visiting Professor)
2003~2004 : University of California at San Diego (Visiting Professor)
2013~2014 : Georgia Institute of Technology(Visiting Professor)