진성 난수 발생기의 성능 검증을 위한 Jitter 분석 방법에 관한 연구

최지우, 박형준, 홍종필

충북대학교

sb7429@chungbuk.ac.kr, phj952000@chungbuk.ac.kr, jphong@chungbuk.ac.kr

A Study on Jitter Analysis Method for Performance Verification of True Random Number Generator

Choi Ji Woo, Park Hyeong Jun, Hong Jong Phil

Chungbuk National Univ.

요 약

본 논문은 링 오실레이터 기반 진성 난수발생기(True Random Number Generator, TRNG)의 성능 검증을 위한 지터(Jitter) 분석 방법을 제안한다. 이 분석 방법은 TRNG의 다양한 아키텍처에 적용 가능하며, 예측 불가능한 지터 성분이 축적되는 과정을 정량적으로 측정하고 분석하여 난수의 엔트로피 수준을 평가하고 진성 난수발생기의 신뢰성을 검증할 수 있다.

Ⅰ. 서 론

진성 난수발생기(True Random Number Generator, TRNG)는 보안 시스템에서 키(Key) 생성을 담당하며 생성된 난수의 엔트로피 수준이 보안 강도를 결정짓는다.

본 논문에서의 링 오실레이터(Ring Oscillator) 기반 진성 난수 발생기는 오실레이터의 발진 과정에서 발생하는 지터(Jitter)를 엔트로피 소스로 활용한다. 지터가 충분히 누적되지 않을 경우 엔트로피 수준이 낮아져 난수 발생기의 성능이 저하될 수 있기 때문에 진성 난수 발생기에서 발생하는 지터를 정량적으로 측정하고 분석하는 방법을 제시한다.

제안하는 방법은 지터를 엔트로피 소스로 활용하는 난수 발생기의 다양한 아키텍처에 적용 가능하며, 예측 불가능한 지터의 축적을 Eye-diagram과 다양한 분포함수(Distribution Function)로 분석하는 방법을 보여준다.

Ⅱ. 본론

2.1 Ring Oscillator 구조

Jitter 특성을 분석하기 위해 사용된 링 오실레이터는 낸드, 인버터, D-Flip-Flop으로 구성되어 있으며, 그림 1과 같이 첫 번째 플립플롭의 클럭 입력으로 링 오실레이터의 출력을 사용하였다.

첫 번째 D Flip-Flop은 Enable 신호가 High가 되었을 때 발진하기 시작하여 지터를 축적하고 발진 횟수에 난수성을 가진다. 두 번째 D Filp-Flop은 FF_CLK 신호가 인가될 때 첫 번째 D Flip-Flop의 랜덤한 출력을 샘플링하여 최종 Output을 출력한다.

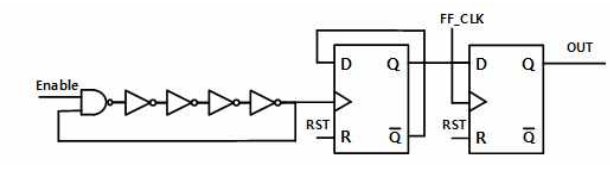

그림 1. Ring Oscillator 구조

2.2 Jitter 성능 분석

지터의 정량적 평가를 위해 Cadence Spectre 시뮬레이션 툴을 사용하여 k 주기 동안 누적된 지터인 Jc(Accumulated jitter)에 대해 분석하였다.

먼저, Jc를 평가하기 위한 첫 번째 방법인 Eye diagram 시뮬레이션이다. 오실레이터의 발진 시간은 각각 10ns와 50ns로 하여 동작시켰고 Eye Period는 오실레이터 출력의 한 주기에 해당하는 0.24n로 설정하였다. 그림 2와 그림 3은 발진 시간에 따른 시뮬레이션 결과이다. 비교 결과, 10ns의 발진 시간을 주었을 때보다 50ns를 주었을 때 Diagram이 균일함을 확인할 수 있다.

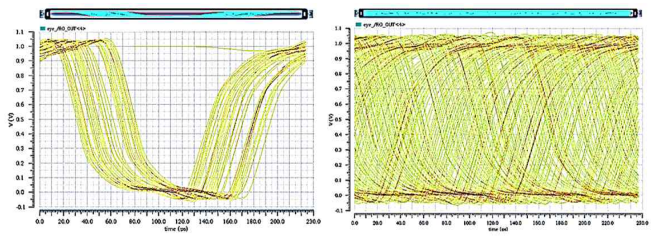

그림 2. 발진 시간 10ns　　그림 3. 발진 시간 50ns

다음은 Spectre의 몬테카를로(Monte Carlo) 시뮬레이션 기능을 활용하여 다양한 k 값에 따른 지터를 분석한 결과이다. 이때 k 값은 측정이 수행되는 주기이자 지터의 축적 시간을 결정하는 변수이다. 시뮬레이션은 ADE Assembler Maestro를 사용하여 진행하였고 몬테카를로는 Process Variation, Random Sampling Method, 1000 Points의 조건에서 수행되었으며, 출력주파수가 3.4[GHz]인 링 오실레이터를 사용하였다.

그림 4는 k 값을 5,000에서 50,000까지 설정하여 시뮬레이션을 수행한 후, 결과를 히스토그램으로 나타낸 것이다. "Plot Histogram-combine" 옵션을 사용하여 4개의 시뮬레이션 결과에서 지터의 분포를 한 번에 확인할 수 있다. 히스토그램의 가로축은 지터 값, 세로축은 샘플 수를 나타낸다. 발진 횟수(k)가 5,000일 때 지터의 평균값이 가장 작고, 샘플이 특정 구간에 집중된 것을 확인할 수 있다. 반면, 발진 횟수가 증가할수록 지터의 평

균값은 커지고, 샘플의 분산도 함께 증가함을 확인할 수 있다.

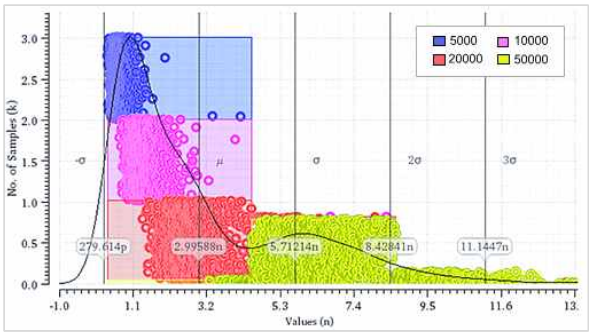

그림 4. k 값에 따른 지터 분포 그래프

다음은 k 값을 1,000에서 100,000까지의 값으로 설정하여 시뮬레이션을 수행한 후에 데이터를 추출하여 표와 정규분포 그래프로 분석한 결과이다. 실제 Chip으로 구현한 진성난수발생기는 발진 시간을 23[us]로 동작시켰을 때 0.97이상의 엔트로피 값을 가졌기에, 이 값을 포함할 수 있도록 80,000이상의 k 값을 포함하였다.

표 1은 다양한 k 값(1000, … , 100000)에 따른 Enable 시간, 지터의 평균값 및 표준편차를 보여준다. 낸드게이트의 입력인 발진 시간(Enable Time)은 수식 (1)과 같이 계산하였다.

$$Enable\ Time = \frac{k}{Ring\ Oscillator\ Frequency} \quad (1)$$

시뮬레이션 결과, k 값이 증가함에 따라 지터의 평균값은 증가하였고 표준편차 역시 증가하는 경향을 보였다. 그림 5는 표 1에 제시된 데이터를 바탕으로, k 값에 따른 지터의 평균(μ)과 표준편차(σ)를 확률밀도함수(Probability Distribution Function, PDF)에 대한 히스토그램으로 시각화한 것이다. 그래프의 가로축은 지터의 평균값이고, 세로축은 평균과 표준편차에 따른 수식 (2)의 값이다. 히스토그램을 통해 k 값이 증가할수록 평균값과 표준편차가 증가하는 경향을 직관적으로 확인할 수 있다.

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

k	Enable[us]	Mean	Std Dev
1,000	0.29	167 p	124 p
5,000	1.47	753 p	173 p
10,000	2.94	1.45 n	286 p
20,000	5.88	2.80 n	532 p
30,000	8.82	4.12 n	778 p
40,000	11.76	5.41 n	1.02 n
50,000	14.71	6.68 n	1.26 n
80,000	23.53	10.4 n	1.98 n
100000	29.41	12.9 n	2.45 n

표 1. k 값에 따른 Enable 시간, 지터의 평균값 및 표준편차

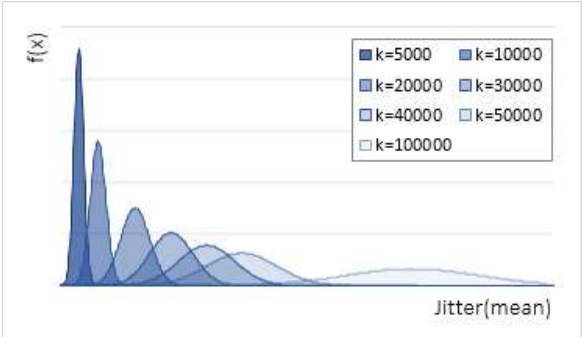

그림 5. k 값에 따른 지터의 가우시안 분포 그래프

특히, k 값이 80,000 이상으로 발진 시간이 23[us]를 초과할 때 지터의 평균값은 10n, 표준편차는 1.98n 이상의 값을 나타냈다. 이처럼 Jc 시뮬레이션을 통해 지터 축적 시간에 따른 난수의 예측 불가능성을 지터의 평균값과 표준편차와 연관 지어 정량적으로 해석할 수 있다.

Ⅲ. 결론

본 논문에서는 링 오실레이터 기반 진성 난수 발생기(TRNG)의 성능을 검증하기 위한 지터(Jitter) 분석 방법을 제시하였다. TRNG의 난수성은 보안 시스템에서 매우 중요한 요소이며, 그 난수성은 링 오실레이터의 발진 과정에서 발생하는 지터의 축적에 의해 결정된다. 이를 검증하기 위해 Cadence Spectre 시뮬레이션 툴을 활용하여 발진 시간에 따른 Eye diagram을 비교하였고, 공정 편차에 따른 지터 특성을 분석하기 위해 몬테카를로(Monte Carlo) 시뮬레이션을 수행하여 결과를 비교 분석하였다.

Jc 분석 결과, 발진 횟수(k 값)가 증가할수록 지터의 평균값과 표준편차가 함께 증가하는 경향을 확인하였다. 이러한 분석을 통해 지터 축적이 TRNG의 난수성에 미치는 영향을 정량적으로 파악할 수 있었으며, 난수 발생기의 최적 발진 시간은 표준편차와 연관지어 해석할 수 있음을 보였다. 이는 오실레이터의 출력주파수가 다른 경우에도 최적의 발진 시간을 찾아낼 수 있는 방법으로, 다양한 TRNG의 성능을 분석하는데 기여할 수 있다.

ACKNOWLEDGMENT

이 논문은 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 지역지능화혁신인재양성사업임 (IITP-2024-2020-0-01462)

이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. 2021R1A2C2005258)

참 고 문 헌

[1] NIST Special Publication 800-90B: Recommendation for the Entropy Sources Used for Random Bit Generation(2018)

[2] K. Yang, D. Fick, M. B. Henry, Y. Lee, D. Blaauw and D. Sylvester, "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), San Francisco, CA, USA, 2014, pp. 280-281, doi: 10.1109/ISSCC.2014.6757434. keywords: {Noise;Generators;System-on-chip;Radiation detectors;Clocks;NIST;Phase frequency detector},

[3] 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