병렬 잡음원 기반 난수발생기에 적합한 엔트로피 건전성 시험

류지은[2], 유현도[2], 강주성[1,2], 염용진[1,2]*
국민대학교 정보보안암호수학과[1] / 금융정보보안학과[2]
{ofryuji, dbguseh111, jskang, *salt}@kookmin.ac.kr

Entropy health test for random bit generator using parallel noises sources

Jieun Ryu[2], Hyeondo Yoo[2], Jusung Kang[1,2], Yongjin Yeom[1,2]*
Dept. of Information Security, Cryptology, and Mathematics[1]/
Financial information security[2], Kookmin Univ.

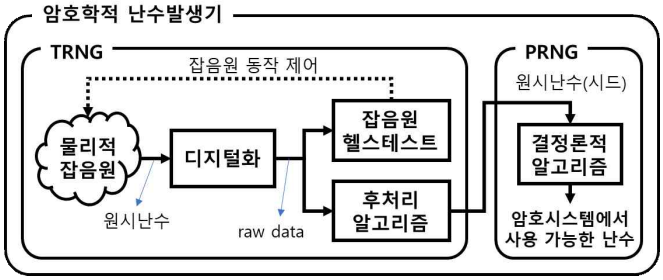
요 약

병렬 잡음원을 사용하는 난수발생기는 빠른 속도로 시드를 생성할 수 있지만, 모든 잡음원에 헬스테스트를 적용하여 각 잡음원이 건전함을 확인해야 한다. 만약 병렬 잡음원에 단일 잡음원에 적용하는 헬스테스트만 적용한다면, 건전하지 않은 잡음원을 빠르게 짚어내고 TRNG 중단을 결정하는 것에 매우 비효율적일 것이다. 따라서 병렬 잡음원 기반 난수발생기는 잡음원 특성에 맞는 헬스테스트를 개발하여 적용할 필요가 있다. 본 논문은 병렬 잡음원 중 하나인 이미지센서를 물리적 잡음원으로 사용하는 난수발생기에 적합한 헬스테스트를 구현하고, 단일 잡음원에 대한 헬스테스트와의 성능을 비교한다. 그리고 성능 비교 결과를 해석하여 병렬 잡음원 사용이 갖는 이점을 제시한다.

Ⅰ. 서 론

난수발생기는 암호키(secret key), 논스(nonce) 등의 생성을 위해 사용되는 암호 시스템의 주요 구성요소 중 하나이다. 이 값들이 알려지면 암호 시스템의 공격으로 이어지기 때문에, 난수발생기의 출력은 예측 불가능성을 가져야 한다.

암호학적 난수발생기는 [그림 1]과 같이 진난수생성기(true random number generator, TRNG)에서 물리적 잡음원으로부터 시드(seed)를 얻고 이를 입력으로 받은 의사난수발생기(psuedo random number generator, PRNG)에서 암호 시스템에서 사용할 긴 길이의 난수를 생성한다. PRNG는 입력된 시드에 대하여 결정론적인(deterministic) 값을 출력하기 때문에 난수발생기의 출력 난수에 대한 예측 불가능성은 시드가 얼마나 예측 불가능한가에 의존한다.



[그림 1] 암호학적 난수발생기의 구조

물리적 잡음원이 고장나면 TRNG의 출력이 0 또는 1 하나의 값만 출력하거나 시드에 일정한 패턴이 나타날 수 있다. 이러한 문제를 방지하기 위하여 물리적 잡음원의 고장 여부를 실시간으로 평가하고 고장난 잡음원을 사용하지 않도록 조치할 필요가 있다.

미국 국립표준 기술연구소(national institute of standards and technology, NIST)는 물리적 잡음원의 고장 여부, 즉 기대하지 않은 값을 출력하는 잡음원을 감지하기 위하여 헬스테스트를 사용하길 권고한다. 그러나 헬스테스트는 난수 생성에는 직접적인 역할을 수행하지 않기 때문에, 난수생성기 성능에 영향을 주지 않을만큼 빠르고 가벼워야 한다. 물리적 잡음원은 종류에 따라 출력 데이터의 특성이 다르기 때문에 헬스테스트는 NIST SP 800-90B를 기반으로 난수발생기가 사용하는 물리적 잡음원에 적합하도록 설계하여 사용한다[1].

한편, 병렬 잡음원을 사용하는 TRNG는 다수의 각 잡음원으로부터 얻은 값으로 시드를 생성한다. 모든 잡음원에 헬스테스트를 적용해야하므로 보다 효율적으로 설계된 헬스테스트가 필요하다. 본 논문에서는 병렬 잡음원인 이미지센서를 물리적 잡음원으로 사용하는 난수발생기에 적합한 헬스테스트를 연구한다. 이미지센서는 각 OBP(optical black pixel)을 잡음원으로 사용하는 병렬 잡음원이다. OBP의 shot noise는 양자적 특성을 보이므로 양자 난수생성기에 사용 가능한 단일 광자 검출기 역할을 대체할 수 있다는 장점을 가진다.

Ⅱ. 병렬 잡음원 기반 난수발생기에 적합한 헬스테스트

1. 헬스테스트 컷오프 설정을 위한 기준

연구에 사용한 이미지센서는 'PV 4209K'로 프레임(frame) 당 540 픽셀, 초 당 7 프레임의 데이터를 전송한다. 각 픽셀이 보내는 데이터는 2 비트로 0, 1, 2, 3 중 하나의 값을 가지며, 이 데이터는 같이 각 프레임으로부터 얻은 값은 2차원 배열에 연속적으로 저장된다.

헬스테스트를 설계하기 위해 OBP가 전송하는 데이터의 특성을 파악하고자 OBP가 전송하는 데이터 값 0, 1, 2, 3의 분포를 확인하였다. 540개 픽셀에 대한 2000 프레임 데이터로부터 얻은 0, 5, 10, 15번째 픽셀의 데이터를 통해 이미지센서의 전체 픽셀이 갖는 데이터 분포를 가정했다. 0과 3의 빈도는 약 $1/6$이고 1과 2의 빈도는 약 $1/3$인 비 균등 분포를 보인다. 이를 기준으로 헬스테스트의 컷오프(cutoff) 값을 결정한다.

2. 개발한 헬스테스트

이미지센서는 병렬 잡음원이므로 각 잡음원에 대한 헬스테스트와 전체 잡음원에 대한 헬스테스트로 나누어 설계한다[2]. [그림 2]는 이미지센서로부터 얻은 데이터를 디지털화하고 픽셀 단위 또는 프레임 단위로 헬스테스트를 수행하는 절차를 나타낸다.

2.1. 각 OBP에 대한 헬스테스트

이는 픽셀 단위로 수행되는 실시간 검사로 두 가지 검정이 있다. 각 픽셀에 대한 테스트는 NIST SP 800-90B에서 제시하는 헬스테스트와 매우 유사하다. 테스트 결과로 실패를 반환한 OBP는 잡음원에서 제외하며, 제외한 OBP 수가 전체 OBP의 20%가 되면 TRNG 동작을 중단한다.

TEST-1) 잡음원 연속 발생 횟수 검정

하나의 OBP가 같은 값을 연속으로 전송한다면 해당 OBP를 잡음원에서 제외한다. 120 프레임을 모니터링하는 동안 15번 연속으로 같은 값이

저장되면 테스트에 실패했다고 판정한다.

TEST-2) 잡음원 편향성 검정

하나의 OBP가 처음 전송한 데이터가 다시 전송되는 횟수를 파악하여 일정 횟수 이상 저장되면 해당 OBP를 잡음원에서 제외한다. 120 프레임을 모니터링하는 동안 60번 이상 같은 값이 전송되면 테스트에 실패했다고 판정한다.

2.2. 전체 OBP에 대한 헬스테스트

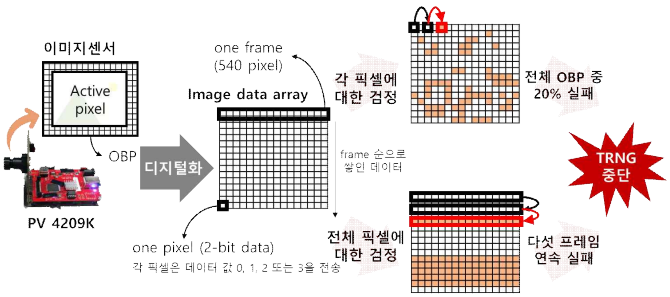
이는 사용자가 요구할 때 프레임 단위로 수행되는 검사로 병렬 잡음원에 특화된 방식의 두 가지 검정이 있다. 두 테스트 모두 5회 연속으로 실패 결과를 반환하면 전체 OBP가 문제가 있다고 판단하여 TRNG 동작을 중단한다.

TEST-3) 잡음원 이진 빈도수 검정

전체 OBP의 출력 데이터가 균등하게 분포되지 않았다면 전체 픽셀이 불건전하다고 판정한다. 저장된 전체 OBP 데이터의 0과 1 빈도수 비율이 5% 이상 차이나면 테스트에 실패했다고 판정한다.

TEST-4) 잡음원 구간 빈도수 검정

전체 OBP의 출력 데이터가 기대하는 분포에 맞는 데이터인지 확인하여 예상 분포와 다르다면 전체 픽셀이 불건전하다고 판정한다. 0과 3은 16.7%, 1과 2는 33.3%를 차지할 것으로 기대하며, 하나의 값이라도 5% 이상 나타나면 테스트에 실패했다고 판정한다.

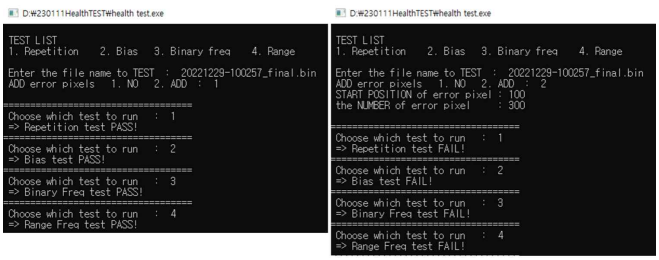


[그림 2] 이미지센서로부터 얻은 데이터에 대한 헬스테스트 적용 과정

Ⅲ. 헬스테스트 구현 결과

각 테스트는 난수 발생기의 효율을 위하여 구조가 단순하고 저장할 변수가 최소한이 되도록 구현한다. TEST-1은 기준 데이터와 반복 횟수를 저장하기 위한 변수 2개, TEST-2는 기준 데이터와 비교 데이터를 저장하기 위한 변수 2개, TEST-3은 0과 1의 개수를 저장하기 위한 변수 2개, TEST-4는 잡음원 데이터 0, 1, 2, 3의 개수를 저장하기 위한 변수 4개를 사용한다.

헬스테스트에 실패하는 경우를 보여주는 실험에는 이미지센서의 고장을 가정하고자 임의 픽셀의 데이터를 전부 0으로 변경하는 과정을 추가하였다. TRNG를 중단시켜야 하는 상황일 때, 테스트 결과로 FAIL이 출력된다. 설계한 헬스테스트를 구현하여 이미지센서로부터 얻은 데이터에 적용한 결과는 [그림 3]와 같다.

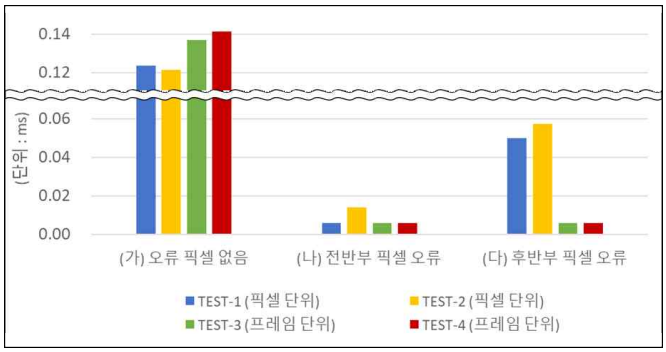


[그림 3] 구현한 헬스테스트 프로그램 동작 예시

구현한 헬스테스트의 성능을 측정하기 위하여, TRNG 동작 중단 명령을 내리기까지 걸리는 시간을 측정했다. 이미지센서의 전체 픽셀 540개 중 (가) 고장 픽셀이 없는 경우와 (나) 10번째 픽셀부터 300개의 픽셀이 고장난 경우, (다) 200번째 픽셀부터 300개 픽셀이 고장난 경우를 나눠 실험했으며, [표 1]은 해당 측정을 천 만 번 수행한 시간의 평균이다.

[표 1] TRNG 동작 중단을 판단하기까지 걸리는 시간 (단위 : ms)

	TEST-1	TEST-2	TEST-3	TEST-4
(가)	1.2×10^{-1}	1.2×10^{-1}	1.3×10^{-1}	1.4×10^{-1}
(나)	5.6×10^{-3}	1.4×10^{-2}	5.6×10^{-3}	5.6×10^{-3}
(다)	5.0×10^{-2}	5.7×10^{-2}	5.7×10^{-3}	5.6×10^{-3}



[그림 4] TRNG 동작 중단을 판단하기까지 걸리는 시간

[그림 4]에서 알 수 있듯 오류 픽셀이 없을 거나 오류 픽셀이 테스트 초반에 발견되는 위치에 있는 경우에는 모든 테스트가 비슷한 속도로 TRNG 동작 중단 여부를 결정한다. 그러나 오류 픽셀이 각 잡음원에 대한 테스트에서 후반에 검사되는 위치에 있는 경우에는 전체 잡음원에 대한 헬스테스트가 훨씬 빠른 속도로 TRNG 동작 중단을 판정한다.

이렇듯 전체 잡음원에 대한 헬스테스트는 병렬 잡음원을 사용하는 TRNG의 동작 중단을 결정하는데 매우 효과적이다. 각 잡음원에 대한 헬스테스트의 경우 하나의 픽셀에 대한 검사를 마친 후 다음 픽셀로 넘어가기 때문에 다수의 픽셀이 고장났다 하더라도 전체 병렬 잡음원의 20%가 고장났음을 확인하려면 고장난 잡음원을 20% 이상 찾을 때까지 시간이 소요된다. 만약 고장난 픽셀이 마지막에 몰려있다면 이 픽셀에 도달할 때까지 TRNG가 중단되지 않을 것이다. 그러나 전체 잡음원에 대한 헬스테스트는 각 잡음원을 하나씩 확인하지 않더라도 한번에 전체 잡음원의 고장 여부를 파악할 수 있어 매우 빠르게 TRNG 동작 중단을 결정할 수 있다.

Ⅳ. 결론

본 논문에서는 병렬 잡음원 기반 난수발생기에 적합한 헬스테스트를 구현하여 헬스테스트가 정상적으로 동작함을 보였다. 또한 병렬 잡음원의 특성을 이용하여 설계된 헬스테스트가 단일 잡음원을 기준으로 설계된 헬스테스트를 사용할 때보다 더 빠르게 병렬 잡음원의 오류 잡음원을 파악하고 TRNG의 동작 중단 여부를 결정할 수 있음을 보였다.

이러한 결과는 병렬 잡음원 기반의 난수발생기가 단일 잡음원 기반의 난수발생기와 비슷한 정도로 건전성을 보장하면서도 보다 빠르게 시드를 생성하도록 만든다. 나아가 병렬 잡음원의 경우 각 픽셀을 병렬 처리할 수 있기 때문에 GPU 구현을 통해 위 속도를 더 단축한다면 단시간에 대량의 난수를 요구하는 환경에서 병렬 잡음원 기반 난수발생기를 더욱 안전하게 사용할 수 있을 것으로 기대한다.

ACKNOWLEDGMENT

이 논문은 2022년도 정부(과학기술정보통신부)의 재원으로 한국연구재단-기후변화대응기술개발 사업의 자원을 받아 수행된 연구임 (No. 2021M1A2A2043893)

참 고 문 헌

[1] M. S. Turan, E. Barker, J. Kelsey, K. A. McKay, M. L. Baish, and M. Boyle, "Recommendation for the Entropy Sources Used for Random Bit Generation," NIST Special Publication 800-90B, Jan. 2018

[2] 유현도, 강주성, 염용진. "경량 암호 CHAM을 사용한 암호학적 난수발생기 GPU 병렬 구현." 한국통신학회 학술대회논문집. (2021): 479-480.

[3] B. K. Park et al., "Practical True Random Number Generator Using CMOS Image Sensor Dark Noise," in IEEE Access, vol. 7, pp. 91407-91413, 2019