하드웨어 잡음원에서 난수성의 검증기준 분석

홍진근*
*백석대학교 정보통신학부
e-mail:jkhong@bu.ac.kr

Verification Criteria Analysis of Randomness in Hardware Noise Source

Jin-Keun Hong*
*Div. of Information and Communication, Baekseok University

요 약

본 논문에서는 하드웨어 잡음원의 난수성에 대한 검증 기준과 관련하여, NIST SP800-22, AIS-31, Crypto-X, FIPS 표준을 기준으로 비교분석하였다.

1. 서 론

난수 발생기에서 하드웨어 잡음원을 이용한 연구는 지속적으로 이루어져 왔다[1-3]. 이러한 연구 배경과 관련하여, Baggini와 Bucci는 백색 잡음의 증폭과 샘플링을 위한 아날로그 및 디지털 컴포넌트의 결합 방식에 대해 연구한 바 있다[4]. 인텔 TRNG는 노이만 교정기와 SHA-1 해쉬 기반의 알고리즘을 적용한 방식을 구현하였고, Fischer와 Drutarovsky는 PLL에 지터를 샘플링 설계에 대한 연구를 수행한 바 있다[5]. 또한 Epstein 등은 메타안정 회로를 기반으로 하는 구조를 제안한 바 있다[6]. 이러한 하드웨어 잡음원을 기반으로 하는 난수발생기의 연구는 그 출력열의 안정성을 보장하기 위한 기본적인 몇 가지의 난수성 검증 테스트를 실시하게 된다. 본 연구에서는 이러한 대표적인 난수성 검증 테스트 방안을 분석하였다.

본 논문에서는 2장에서 잡음원 출력열의 난수성 검증 기준을 제시하였고, 3장에서 TRNG별 난수성 테스트 기준을 언급하고, 4장에서 결론을 맺었다.

2. 잡음원의 출력열 난수성 검증 기준

1) NIST 800-22 기준

NIST 800-22는 A statistical test suite for random and pseudo-random number generator for cryptographic application 주제를 다룬다. 통계적 테스트 슈트는 난수 테스팅에 대한 개요(랜덤성, 불예측성, 실난수발생기, 의사난수발생기, 테스팅, 난수성 및 불예측성과 테스팅에 대한 고려사항), 난수 발생 테스트(주기성, 블록 내 주기성, 런 테스트, 블록내 1의 최장 런 수 테스트, 이진 메트릭스 랭크 테스트, DFT 테스트, 오버랩 되지 않은 템플레이트 매칭 테스트, 오버래핑되는 템플레이트 매칭 테스트, 마우어 유니버설 통계 테스트, 선형 복잡도 테스트, 시리얼 테스트, 근사 엔트로피 테스트, 누적 합(cusum) 테스트, 랜덤 이탈성 테스트, 랜덤 이탈의 변형성 테스트), 테스트의 기술적인 설명, 테스팅 전략과 결과 해석, 사용자 가이드, 부록(소스코드), 등으로 구성된다.

- Frequency Test
- Cumulative Sum Test
- Runs Test
- Rank Test
- Spectral Test
- Templates Matching Test
- Universal Statistical Test (Maurer)
- Approximate Entropy Test (Pincus & Singer)
- Random Excursions Test
- Moving Averages Test
- Lempel-Ziv Compression Test
- Linear Complexity Test
- Bayes Test

그림1에서, 제시된 AES 랜덤성 테스트 사례는 통계적 테스트 각 항목에서 요구되는 P 값에 대한

참조 값을 언급한 것이다.

Statistical Test	No. of P-values	Test ID	Statistical Test	No. of P-values	Test ID
Monobit	1	1	Periodic Template	1	157
Block Frequency	1	2	Universal Statistical	1	158
Cusum	2	3-4	Approximate Entropy	1	159
Runs	1	5	Random Excursions	8	160-167
Long Runs of Ones	1	6	Random Excursions Variant	18	168-185
Rank	1	7	Serial	2	186-187
Spectral DFT	1	8	Lempel-Ziv Compression	1	188
Aperiodic Templates	148	9-156	Linear Complexity	1	189

[그림1] AES 랜덤성 테스트 예

또한 그림2에서 제시한 바와 같이, 랜덤성의 확률분포와 길이 값을 테스트 항목별로 나타낼 수제시하였다.

Test	Reference distribution	Recommended size (bits)
1. Frequency (monobits)	half-normal	$n \geq 100$
2. Frequency (blocks)	χ^2	$n \geq 100$
3. Runs	χ^2	$n \geq 100$
4. Longest run of ones (block)	χ^2	$n \geq 128$ up to 750000
5. Binary Matrix Rank[2]	χ^2	$n \geq 38912$
6. Discrete Fourier Transform	normal	$n \geq 1000$
7. Non-overlapping Template Matching	χ^2	$n \geq 10^6$
8. Overlapping Template Matching	χ^2	$n \geq 10^6$
9. Maurer's	half-normal	$n = 387840$ up to 10^9
10. Lempel-Ziv Compression	normal	$n \geq 10^6$
11. Linear Complexity	χ^2	$n \geq 10^6$
12. Serial[1]	χ^2	$m \leq \lfloor \log_2(n) \rfloor - 2$
13.Approximate Entropy[1]	χ^2	$m \leq \lfloor \log_2(n) \rfloor - 2$
14. Cumulative Sums	normal	$n \geq 100$
15. Random Excursions	χ^2	$n \geq 10^6$
16. Random Excursions Variant	half-normal	$n \geq 10^6$

[그림2] 랜덤성 확률분포와 길이

제시된 테스트 항목을 랜덤 관점, 패턴 관점, 복잡도와 압축 관점에서 분류해보면 표1에서와 같이 나타낼 수 있다.

[표 1] 랜덤성 테스트 항목 특성분류

랜덤관점에서 스트링	패턴 관점		복잡도/압축
주기	런	롱런	랭크
블록주기	비주기 템플레이트	유니버설 통계성	스펙트럴
누적 합	주기적 템플레이트	시리얼	Lempel-Ziv 복잡성
랜덤 이탈성(변형)	근사 엔트로피		선형복잡도

2) AIS-31 기준

AIS-31 물리적 랜덤 난수 발생기를 위한 기능적 클래스 및 평가 방법에 대한 연구를 W. Killmann과 W. Schindler가 수행한 바 있다. AIS-31은 TRNG를 위한 평가 기준을 제시하고 있는데, 온라인 통계적 테스트를 정의하고 있으며, TRNG가 정상적으로 동작하는지를 검증할 목적으로 수행된다. TRNG 응용과 관련하여, P1은 CR 프로토콜이나 개방된 전송, 일정하지 않은 초기치 벡터, K1등급이나 K2 등급의 PRNG를 위한 시드 생성에 사용된다. P2 등급은 서명키 쌍의 생성이나 DSS 서명의 생성, 대칭형 암호 메커니즘을 위한 세션 키의 생성, 랜덤 패딩 비트, 영지식 증명, K3와 K4 등급의 PRNG를 위한 시드 생성에 적용된다. AIS-31 테스트는 P1, P2 특성을 검증하기 위해 통계적 검증을 실시하며, 테스트는 T1-T4와 T5(AIS-20)가 실시된다.

- T0: Disjointness test
- T1: Mono bit test
- T2: Poker test
- T3: Run test
- T4: Long run test
- T5: Autocorrelation test
- T6: Uniform distribution test
- T7: Comparative test for multi nomial distribution
- T8: Entropy test

3) Crypto-X 기준

스트림 암호에 대한 테스트 기준은 다음과 같다.

- Frequency
- Binary Derivative
- Change Point
- Runs
- Sequence Complexity
- Linear Complexity
- Key Generator Tests

키 수열 발생기에 대한 테스트 기준은 다음과 같다.

- Frequency
- Binary Derivative
- Sub-blocks
- Entropy

블록암호에 대한 테스트 기준은 다음과 같다.

- Frequency
- Binary Derivative
- Sub-blocks
- Avalanche Criteria
- Avalanche Variable

그림3에서는 RC4 알고리즘 출력 열에 대한 Crypt-X의 테스트 검증 기준이다.

	Number of p-values less than:		
Test	***.10***	***.05***	***.01***
Frequency	6	4	3
Binary Derivative (1)	8	6	2
Binary Derivative (2)	11	7	1
Change Point	24	13	5
Subblock (b = 4)	9	3	0
Subblock (b = 8)	9	6	1
Subblock (b = 16)	13	5	1
Subblock (b = 30)	9	4	0
Runs Distribution	5	3	2
Longest Run	Max = 33	Next = 28	
Linear Complexity	5	5	1
LC profile - Jumps	12	8	0
LC Profile - Jump Size	20	13	3
Sequence Complexity	Max = 6143	Min = 6110	

[그림3] RC4의 Crypt-X 테스트 기준

4) 다이하드 기준

- Birthday Spacings Test
- Overlapping 5-permutation Test
- Binary Rank Test for Matrices 31x31 & 32x32
- Binary Rank Test for 6x8 Matrices
- Count the Number of 1''s in a stream of bytes
- Count the Number of 1''s in specific bytes
- Monkey tests on 20-bit words
- Monkey tests on OPSO
- Monkey tests on OQSO
- Monkey tests on DNA
- Parking Lot Test
- Overlapping Sums Test
- Squeeze Test
- Minimum Distance Test
- Random Sphere's Test

5) FIPS 140-1/-2 기준

- Monobit test, Poker test, Run test, Long run test

3. TRNG별 난수성 테스트 기준

표2에서는 TRNG 유형별로 난수성 테스트 기준을 제시하고 있다.

[표 2] TRNG 유형별 테스트 기준

IQ Quantique Quantis	NIST & DIEHARD
SafeXcel IP TRNG	FIPS 140-2
ID Quantique	NIST & DIEHARD
HG324	NIST & DIEHARD
Araneus Alea I	NIST & DIEHARD
Zrandom USB	DIEHARD &POKER
Protego R200/210/230	Crypt-X
Comscire J1000KU	J-S Coron
Orion Products	256bit run test

4. 결 론

본 논문은 TRNG 출력열의 검증하는데 요구되는 주요 난수성 검증 방식에 대한 분석이다. 이 테스트 기준은 NIST 800-22 기준을 따르거나, AIS-31, Crypto-X, 다이하드 기준을 수용하여 적용하고 있다. TRNG 난수 발생기의 출력열 난수성 테스트 기준 가운데 보편적으로 적용되는 기준이 NIST 800-22 기준이나 다이하드 기준이다.

참고문헌

[1] W. Schindler and W. Killmann, "Evaluation Criteria for TRBG used in cryptographic applications," CHES2002, LNCS2523, pp.431-449, August 2002.

[2] Marsalglia, G. DIEHARD: A Battery of Tests of Randomness, http://stat.fsu.edu /geo, 1996.

[3] NIST Special Publication 800-22, "A statistical test suite for random and pseudo random numbers," Dec. 2000.

[4] Vittorio Bagini, and Marco Bucci A Design of Reliable True Random Number Generator for Cryptographic Applications. CHES1999, pp. 204-218, LNCS1717 1999.

[5] Viktor Fischer, and Miloˇs Drutarovsky, " True Random Number Generator Embedded in Reconfigurable Hardware," CHES 2002, pp.415 - 430, LNCS 2523 2003.

[6] Michael Epstein, Laszlo Hars, Raymond Krasinski, Martin Rosner, and Hao Zheng, "Design and Implementation of a True Random Number Generator Based on Digital Circuit Artifacts," CHES 2003, pp. 152 - 165, LNCS 2779.