Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.1, Feb. 2016 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.1.49

진난수발생기용 난수성 검정 방법 AIS.31에 대한 확률론적 분석 및 보안성 평가 적용 방법*

박 호 중,† 강 주 성,‡ 염 용 진
국민대학교 수학과 / 금융정보보안학과

Probabilistic Analysis of AIS.31 Statistical Tests for TRNGs and Their Applications to Security Evaluations*

Hojoong Park,† Ju-Sung Kang,‡ Yongjin Yeom
Dept. of Math. / Financial Information Security, Kookmin University

요 약

진난수발생기(TRNG)의 통계적 난수성을 평가하는 대표적인 방법으로 미국 NIST의 SP 800-90B와 독일 BSI의 AIS.31을 들 수 있다. 본 논문에서는 현재 국제 표준화 작업이 진행 중인 독일 BSI의 AIS.31에 집중하여 세부 내용을 분석한다. AIS.31 문서에 나타나 있는 통계적 검정 방법들을 확률론적으로 면밀히 분석하여 각 통계량의 분포와 그 의미를 밝혀내고, 유의수준과 표본수열의 길이에 따른 검정 통과 기준을 제시함으로써 AIS.31을 일반화한 결과를 도출한다. 또한, AIS.31에서는 정확히 기술하고 있지 않은 검정의 반복 시행 결과들에 대해 신뢰구간 개념을 적용한 최종 통과 기준을 제안하고, 적절한 시뮬레이션을 통하여 본 논문의 분석 결과에 대한 유효성을 확인한다.

ABSTRACT

SP 800-90B of NIST(USA) and AIS.31 of BSI(Germany) are representative statistical tests for TRNGs. In this paper, we concentrate on AIS.31 which is under the ongoing international standardization process. We examine the probabilistic meaning of each statistic of the test in AIS.31 and investigate its probability distribution. By changing significance level and the length of sample bits, we obtain formalized accept region of the test. Furthermore we propose the accept regions for some iterative tests, that are not mentioned in AIS.31, and provide some simulations.

Keywords: Statistical test, AIS.31, True random number generator

I. 서 론

암호학적 난수발생기는 크게 진난수발생기(true random number generator)와 의사난수발생기(pseudo-random number generator)로 구분할 수 있다. 지금까지 난수발생기에 대한 안전성 평가는 주로 암호 모듈내의 난수발생기나 의사난수발생기에 대해서 이루어져 왔다. 암호모듈에 대한 안전성 평가를 다루고 있는 미연방 표준 FIPS 140-1[4]과 140-2[5]에는 암호모듈 내부의 난수발생기에 대한 안전성 평가 부분이 포함되어 있다. 미국 NIST의 SP 800-22[6]와 독일 BSI의 AIS.20[3] 문서는 의사난수발생기에 대한 통계적 난수성 평가를 위해 알려진 대표적인 방법들이다. Table 1.에는 AIS.31, FIPS 140, SP 800-22, SP 800-90B 등에 대한 간단한 비교가 나타나 있다. NIST의 SP

Received(09. 18. 2015), Modified(10. 28. 2015), Accepted(12. 09. 2015)
* 본 연구는 2015년도 정부(미래창조과학부)의 재원으로 한국연구재단-차세대정보·컴퓨팅기술개발사업의 지원을 받아 수행된 연구임(No. 2014M3C4A7030648)
† 주저자, ruokay@kookmin.ac.kr
‡ 교신저자, jskang@kookmin.ac.kr(Corresponding author)

Table 1. Comparing AIS.31, FIPS 140, SP 800-22 and SP 800-90B

	AIS.31	FIPS 140	SP 800-22	SP 800-90B
Purpose	Evaluation criteria for true random number generator.	Security require-ments that are to be satisfied by a cryptographic module.	Randomness of RNG and PRNG is required for cryptographic purposes.	Specify the design and testing require-ments for entropy sources that can be validated as appro-ved entropy sources by NIST's CAVP and CMVP.
Test	·**T0** : Disjointness test ·**T1** : Monobit test ·**T2** : Poker test ·**T3** : Run test ·**T4** : Longrun test ·**T5** : Autocorrelation test ·**T6** : Uniform distribution test ·**T7** : Comparative multinomial test ·**T8** : Entropy test	**Statistical test of FIPS 140-1** ·Monobit test ·Poker test ·Run test ·Longrun test	·15 Statistical Test	·**IID Test** · 6 Shuffling test · 2 Specific statistical test ·**5 Non-IID Test**
Significance level	10^{-6}	10^{-4}	10^{-2}	10^{-3}
Relation	◎ Statistical test of FIPS 140-1 is same to T1~T4 of AIS.31. ◎ AIS.31 is similar to 800-22, but significance level of 800-22 is more stronger than AIS.31. ◎ Target of evaluation of AIS.31 and 800-90B is same as intermediate output bits. ◎ The purpose of 800-90B and statistical tests of FIPS 140-1 is same. ◎ For autonomy of evaluation group, Statistical test is deleted in FIPS 140-2.			

800-22가 공개된 이후로 의사난수발생기에 대한 통계적 검정 방법에 관한 연구는 어느 정도 안정기에 접어들었다고 할 수 있다. 이러한 배경을 바탕으로 최근에는 진난수발생기의 안전성 평가에 대한 학계와 산업계 및 공공 기관의 논의가 활발히 진행되고 있는 상황이다.

현재 드래프트(draft) 상태에 놓여있는 NIST의 SP 800-90B[7] 문서는 정보이론을 근간으로 한 엔트로피(entropy)에 기반을 둔 측도(measure)를 사용하여 진난수발생기의 안전성을 평가하고자 하는 노력을 보여주고 있다. 독일 BSI는 기존의 통계적 난수성 검정 방법에서 크게 벗어나지 않은 것으로 보이는 AIS.31[1]을 제안하여 이를 진난수발생기 평가에 대한 ISO 국제 표준으로 제정할 것을 추진 중에 있다. 본 논문에서는 개략적인 내용과 검정 방법들의 통과 범위만 제시되어 있는 AIS.31 문서를 면밀히 분석하여 그 이론적 배경을 확실히 하고, 실제로 진난수발생기 평가에 AIS.31 기준을 적용할 때 발생 가능한 문제점들과 이에 대한 해결책을 모색하고자 한다.

1.1 AIS.31 온라인 평가 기준의 일반화

AIS.31 평가 기준의 본래 목적은 진난수발생기의 작동 중에 내부난수의 완전붕괴를 검출하기 위한 것으로 이것을 온라인 검정이라 한다. 이 온라인 검정을 아무런 수정 사항 없이 오프라인 검정에 그대로 적용하는 것은 여러 가지로 무리가 있다. 그러므로 온라인 검정에서 제시하고 있는 기준들을 이론적으로 명백히 분석하여 오프라인 검정에도 적용할 수 있도록 확장하는 것이 중요하다.

최근 주목받고 있는 임베디드와 모바일 환경에 사

용되는 보안제품에서도 안전성 높은 난수발생기는 필수 요소이다. 이러한 임베디드와 모바일 환경의 장비들은 그 특성에 따라 잡음원 확보의 용이성 또한 다양할 수밖에 없다. 그러므로 장비별 특성에 따른 다양한 잡음원으로부터 추출된 정보를 입력으로 한 진난수발생기 출력 수열의 난수성 평가 방법을 획일적으로 적용하는 것은 바람직하지 못하다. 난수성을 보장하는 최소한의 평가 기준으로 볼 수 있는 AIS.31의 검정 통과 범위를 다양한 환경에 부합하는 합리적인 기준으로 일반화 한다면 매우 유용할 것이다.

1.2 주요 결과 및 활용 방안

본 논문에서는 독일 BSI의 AIS.31 문서에 나타나 있는 통계적 검정 방법을 확률론적으로 면밀히 분석하여 AIS.31의 기준을 일반화 하고, 이를 다양한 환경 하에서의 진난수발생기에 대한 온라인 및 오프라인 난수성 평가에 실제로 적용할 때 고려해야 할 사항들에 대한 해결책을 제시한다. 논문에 나타나 있는 연구 결과를 요약하면 다음과 같다.

- AIS.31 문서에 나타나 있는 통계적 검정법에 대한 확률론적 분석을 통하여 각 통계량(statistic)을 수식화 하고, 검정 방법에 내재되어 있는 확률론적 극한 정리를 밝혀낸다.
- 확률론적 분석 내용을 바탕으로 유의수준(significance level)과 표본수열의 길이에 따른 AIS.31 통계적 검정법의 일반화된 통과 기준을 도출해낸다.
- 신뢰구간(confidence interval) 개념을 사용하여 일반화된 AIS.31 통계적 검정을 반복적으로 시행할 수 있는 환경에서 필요로 하는 최종 통과 기준을 제안한다.
- 독일의 BSI에서 제공한 AIS.31 JAVA 소스코드[14]를 분석하여 일반화된 버전으로 수정한 프로그램을 구동시킴으로써 얻을 수 있는 다양한 시뮬레이션 결과를 제시한다.

이러한 연구 결과는 난수성 평가를 요하는 실용적인 환경에서 여러 가지 활용 방안을 생각해볼 수 있다. 우선적으로 적용 가능한 방안을 고려하면 다음을 들 수 있다.

- 일반화된 검정 기준을 적용함으로써 AIS.31에서 2만 비트로 고정되어 있는 표본의 길이를 가변적으로 조절하여 통계적 검정을 실시할 수 있다.
- 대용량의 표본이 주어지거나 잡음원 수집이 어려운 환경에서는 검정을 반복 시행할 때의 최종 통과 기준을 적용하여 난수성을 평가할 수 있다.
- 유의수준 변화에 따른 검정 통과 여부나 반복 시행 시의 최종 통과 여부를 비교함으로써 보안제품의 난수성에 대한 우열을 평가하는 데 활용 가능하다.

II. AIS.31 통계적 검정법 소개

2.1 AIS.31 문서개요

AIS.31[1] 문서에서는 진난수발생기(TRNG)의 내부 중간 단계에서 추출 가능한 상태의 난수를 평가하는 기준을 제시하고 있다. 진난수발생기의 중간단계는 Fig.1.에서와 같이 디지털화된 잡음원과 내부난수로 나눌 수 있다. AIS.31에서는 내부난수를 클래스 P1에 속하는 단계로 분류하여 6가지 검정법으로 평가하고, 디지털화된 잡음원에 대해서는 클래스 P2에 속하는 단계로 분류하여 3가지 검정법으로 평가할 것을 권고하고 있다.

클래스 P1은 6가지 검정법을 통과한 내부난수를 의미한다. 클래스 P1에 적용되는 검정 방법에는 T0부터 T5까지로 명명된 6가지 검정법이 포함된다. T0은 불일치(disjointness) 검정, T1은 모노비트(monobit) 검정, T2는 포커(poker) 검정, T3는 런(run) 검정, T4는 롱런(long run) 검정, T5는 자기상관관계(autocorrelation) 검정법으로 불린다. 여기에서 T0은 이 검정을 통과하는 경우 다음 검정을 진행할 수 있는 예비검사성격을 지니고 있다. T0을 제외한 T1부터 T5까지의 검정에 대해서는 표본수열의 길이를 2만 비트로 설정하고, 유의수준 α는 10^{-6}으로 고정하고 있다. T0 검정을 통과한 내부난수가 이후의 5가지 검정법을 257번 반복 수행한 검정을 모두 통과하는 경우에 이 내부난수는 클래스 P1에 속하는 것으로 판정된다.

클래스 P2에 적용되는 검정 방법에는 T6, T7, T8이 속하고, 이들은 각각 균일분포(uniform

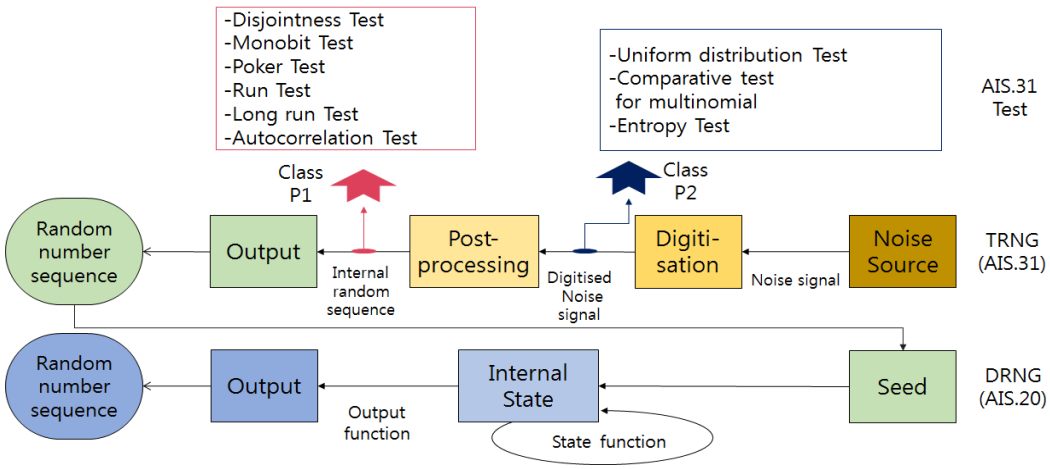

Fig. 1. Step of AIS.31

distribution) 검정, 다항분포 검정(comparative test for multinomial), 엔트로피(entropy) 검정이다. AIS.31 문서에서는 T6의 세부 검정법 2가지, T7의 세부 검정법 2가지에 T8을 포함한 5가지 검정법을 10만 비트 이상의 표본수열에 적용한 결과를 바탕으로 검정 통과 여부를 판정한다. 표본수열이 5가지 검정 기준을 모두 만족하면 클래스 P2에 속하는 것으로 판정된다. 만일 5가지 검정법 중 2가지 이상을 통과하지 못하는 표본수열은 클래스 P2에 속하지 않는 것으로 판정된다. 그리고 5가지 중 어떤 하나의 검정 기준만을 통과하지 못하는 경우에는 추가적인 검정을 실시한다. 단 한 번의 추가적인 검정에서 5가지 모두를 통과하는 경우에는 클래스 P2에 속하는 것으로 판정하고, 그렇지 않은 경우에는 검정 실패로 판정한다.

2.2 AIS.31의 검정 방법 요약

AIS.31 통계적 검정 원리는 '표본수열이 랜덤하다'를 귀무가설 H_0으로 설정 하고, '표본수열이 랜덤하지 않다'를 대립가설 H_1로 설정하여 H_0에 대한 반증을 찾아내고자 하는 가설검정법이다. 가설검정법은 반증을 찾아내는 과정에서 유의확률(p-value)을 계산하여 표본의 유의성을 밝혀내기 때문에 유의성 검증이라고도 한다. 표본이 랜덤하다는 의미는 표본수열의 각 비트가 서로 독립이고 동일한 균일 분포를 보인다는 것이다. 유의확률의 계산 값이 유의수준 α 보다 큰 표본수열은 랜덤한 것으로 판정된다. 즉,

$$P-value > \alpha \quad \Rightarrow \quad \text{표본수열은 랜덤하다.}$$

AIS.31의 검정법은 총 9가지의 검정으로 구성된다. 그 중 포커와 다항분포 검정은 카이제곱검정(적합도 검정)을 통해 통과 기준을 주고, 모노비트, 런, 자기 상관관계, 균일분포, 엔트로피 검정은 정규분포의 오류함수(error function)를 이용하여 통과 기

Table 2. Statistical tests of AIS.31

Test	Mean
T0 (Disjointness)	Subsequent members are pairwise different.
T1 (Monobit)	Uniform test for bit sequence of length 20,000
T2 (Poker)	Goodness of fit test for the number of 4 bits block.
T3 (Run)	Test for the number of run which has l-length.
T4 (Longrun)	Check up the occurrence run of length ≥ 34.
T5 (Autocorrelation)	Autocorrelation value of $\sum(i\text{-th bit} \oplus i+5000\text{-th bit})$ which is approximately 2500
T6 (Uniform distribution)	Uniform distribution test using ratio of 0's and 1's.
T7 (Comparative test for multinomial)	Goodness of fit test for h blocks by comparison.
T8 (Entropy)	Estimate entropy as minimum distance of blocks.

준을 제공한다. Table 2.는 AIS.31의 검정법 종류와 간단한 설명이다. 검정에 대한 자세한 설명은 다음 장에서 다룬다.

III. AIS.31의 확률론적 분석 및 일반화

표본수열이 랜덤하다는 의미는 각 비트가 서로 독립이고, 0과 1의 발생 확률이 각각 1/2이라는 것이다. 랜덤한 표본수열은 독립 반복 시행의 결과이므로 길이가 n인 표본수열은 확률론적으로 이항분포를 따른다. 그런데 AIS.31의 검정 통계량은 정규분포와 카이제곱분포를 따르는 것으로 기술되어 있다. 우리는 이항분포에서 출발하여 정규분포와 카이제곱분포가 도출되는 과정을 확률론적으로 분석하고자 한다.

정규분포를 따르는 검정 통계량의 경우에는 통과 기준이 유의수준 α와 표본수열의 길이 n에 영향을 받는다. 랜덤한 표본수열은 이항분포를 따르지만, n이 큰 수일 경우에는 관련 확률값을 계산하는 것이 어렵기 때문에 확률론의 극한정리를 이용하여 상대적으로 편리한 정규분포를 이용하는 것이 일반적이다. 길이가 n인 랜덤한 표본수열에서 1의 개수를 나타내는 확률변수를 X라 하면, 이는 평균과 분산이 각각 $E[X]=\mu_X=n/2$, $Var[X]=\sigma_X^2=n/4$ 인 이항분포를 따른다. 그런데 충분히 큰 n에 대하여 X의 분포는 정규분포로 근사한다는 사실이 알려져 있다[15]. 즉,

$$X\sim B\left(n,\frac{1}{2}\right)\approx N\left(\frac{n}{2},\frac{n}{4}\right) \quad .$$

정규분포를 따르는 경우 오류함수(error function)를 사용하여 통과 기준을 구하게 된다. 오류함수는 정규분포함수의 양쪽 끝 부분의 넓이를 나타내고자 하는 것으로 유의확률을 구하고자 할 때 사용된다. 정규분포의 오류함수는

$$\Phi(z)=\frac{2}{\sqrt{2\pi}}\int_z^{\infty}e^{-x^2/2}dx$$

로 정의된다. 이때, 유의수준 α에 따른 z값은 다음과 같이 구할 수 있다.

$$\Phi(z)=\frac{2}{\sqrt{2\pi}}\int_z^{\infty}e^{-x^2/2}dx=\alpha \qquad (1)$$

아래 표는 본 논문에서 주로 사용하는 유의수준 α에 따른 z값을 작성한 것이다.

Table 3. Values of z corresponding to α

Significance level	10^{-3}	10^{-4}	10^{-5}	10^{-6}	10^{-7}
z	3.29	3.89	4.42	4.89	5.33

일반적인 정규분포는 표준정규분포로 변환이 가능하다. 그러므로 Table 3.에 나타나 있는 z값을 검정 과정에 이용하기 위하여 다음과 같은 수식을 고려한다. 양수 z와 $\sigma_X=\sqrt{Var(X)}$ 에 대하여,

$$\begin{aligned}&P(-z<Z<z)\\&=P\left(-z<\frac{X-\mu_X}{\sigma_X}<z\right)\\&=P(\mu_X-z\sigma_X<X<\mu_X+z\sigma_X)\\&=P\left(\frac{n}{2}-z\sqrt{\frac{n}{4}}<X<\frac{n}{2}+z\sqrt{\frac{n}{4}}\right)\end{aligned} \qquad (2)$$

이 성립한다.

검정 통계량이 카이제곱분포를 따르는 경우에는 통과 기준이 자유도 d와 유의수준 α에 영향을 받는다. 이 경우에는 단측검정을 실시하는 것이 일반적이다. 카이제곱분포의 오류함수는

$$\Phi(y)=\left[\Gamma\left(\frac{d}{2}\right)2^{d/2}\right]^{-1}\int_y^{\infty}x^{(d-2)/2}e^{-x/2}dx$$

이다. 이때 유의수준 α에 따른 y는 다음과 같이 구할 수 있다.

$$\begin{aligned}\Phi(y)&=\left[\Gamma\left(\frac{d}{2}\right)2^{d/2}\right]^{-1}\int_y^{\infty}x^{(d-2)/2}e^{-x/2}dx\\&=\alpha\end{aligned} \qquad (3)$$

식 (3)에서 Γ는 특수함수인 감마함수를 의미한다.

3.1 클래스 P1

내부난수가 클래스 P1에 속함을 보장해주는 통계적 검정으로는 불일치, 모노비트, 포커, 런, 롱 런, 자기 상관관계 검정이 있다. 이 6 가지 검정 방법 중 예비 검사 성격을 가진 불일치 검정은 유의수준 α를 2^{-17}, 표본수열의 길이를 48 비트인 블록 2^{16}

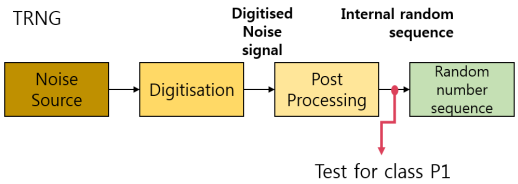

Fig. 2. Test for class P1

개 총 3,145,728 비트로 고정하고 있다. 반면에 나머지 5 가지 검정 방법은 표본수열의 길이 n 이 2만 비트, 유의수준 α 가 10^{-6}으로 고정되어 있다. 본 소절에서는 기존 클래스 P1의 검정법 6 가지를 분석하고 표본수열의 길이 n 과 유의수준 α 를 변화시켜 일반화된 통과 기준을 제시한다.

3.1.1 불일치 검정

불일치 검정의 표본은 48비트인 2^{16}개의 블록이다. 이 검정 방법은 임의의 두 블록이 같은 값을 가지는 경우를 확인하는 검정으로 불일치 검정을 통과해야만 다음 검정이 진행될 수 있는 예비 검사 성격을 지니고 있다. 임의의 블록을 $w_i \in \{0,1\}^{48}$라 하면 한 블록 w_i에서 발생할 수 있는 비트의 모든 블록의 수는 2^{48}이다. 두 블록이 같은 값으로 충돌하는 경우는 블록 2^{16}개에서 같은 값을 가지는 블록 2개를 선택하는 사건으로 표현할 수 있다. 이를 수식으로 표현하면

$$\binom{2^{16}}{2} = \frac{2^{16}(2^{16}-1)}{2}$$

이다. 이 때 충돌이 발생할 확률은

$$\frac{2^{16}(2^{16}-1)/2}{2^{48}} \approx \frac{2^{31}}{2^{48}} = \frac{1}{2^{17}}$$

이다.

AIS.31에 제시된 불일치 검정은 블록의 길이와 개수를 변화시키는 방법으로 유의수준을 일반화시킬 수 있다. 불일치 검정의 블록의 길이를 l, 블록의 수를 2^y으로 설정하였을 때, 충돌 확률의 일반화된 수식은

$$\frac{1}{2^l}\binom{2^y}{2} = \frac{2^y(2^y-1)/2}{2^l} \approx \frac{2^{2y}}{2^{l+1}} = 2^{2y-(l+1)}$$

이다. 위의 수식을 이용하여 블록 길이 l과 블록의 수 2^y을 변화시켜 불일치 검정을 적용하고자 할 때 필요한 두 변수 사이의 관계는 Table 4.와 Table 5.에 예시적으로 나타나 있다.

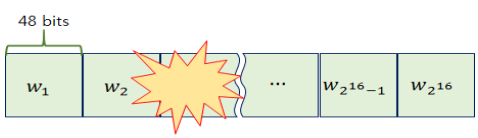

Fig. 3. Disjointness test

Table 4. The number of blocks 2^y corresponding to l when significance level is 2^{-17}

The length of a block l	40	44	48	52
The number of blocks 2^y	2^{12}	2^{14}	2^{16}	2^{18}

Table 5. The number of blocks 2^y corresponding to some significance level when the length of a block is 48 bits.

Significance level	2^{-13}	2^{-16}	2^{-20}	2^{-23}
The number of blocks 2^y	2^{18}	2^{17}	2^{15}	2^{13}

3.1.2 모노비트 검정

모노비트 검정은 표본수열에서 0과 1이 균등하게 나타나는지 확인하는 검정 방법으로 표본수열에서 1의 개수의 분포로 난수성을 검정한다. 이 검정에서 길이가 2만 비트인 랜덤한 표본수열에서 1의 개수를 나타내는 확률변수를 X라 하면, X는 평균이 10000, 분산이 5000인 이항 분포를 따르고, 2만은 충분히 큰 수이기 때문에 X의 분포는 정규분포로 근사한다[10]. 즉,

$$X \sim B(20000, 1/2) \approx N(10000, 5000).$$

또한 AIS.31에 제시된 모노비트 검정의 유의수준 α는 10^{-6} 이므로 Table 2.를 통해 $z \approx 4.89$ 를 얻을 수 있고, 이 z 값과 평균 및 분산을 수식 (2)에 적용하면 통과 기준

$$9654 < X < 10346$$

을 구할 수 있다.

모노비트 검정의 일반화된 통과 기준은 표본수열

의 길이 n 과 유의수준 α 를 변화시키는 방법을 사용한다. 표본수열의 길이를 n으로 설정하면, 평균과 분산이 각각 $\mu_X = n/2$, $\sigma_X^2 = n/4$인 이항 분포를 따르고, 충분히 큰 n에 대해서 X는 정규분포로 근사한다.

$$X \sim B\left(n, \frac{1}{2}\right) \approx N\left(\frac{n}{2}, \frac{n}{4}\right).$$

그리고 유의수준 α 에 대응하는 z 값을 수식 (1)을 이용하여 구하고, μ_X와 σ_X 값을 수식 (2)에 대입하면 통과 기준을 일반화 할 수 있다. 모노비트 검정을 일반화시킨 통과 기준을 Table 6.에 제시한다.

Table 6. Accept regions of monobit test

Significance level $\alpha = 10^{-4}$	
Length of n	Accept region
2×10^4	$9724 < X < 10276$
4×10^4	$19611 < X < 20389$
8×10^4	$39449 < X < 40551$
10^6	$498055 < X < 501945$

Significance level $\alpha = 10^{-5}$	
Length of n	Accept region
2×10^4	$9687 < X < 10313$
4×10^4	$19558 < X < 20442$
8×10^4	$39374 < X < 40626$
10^6	$497790 < X < 502210$

Significance level $\alpha = 10^{-6}$	
Length of n	Accept region
2×10^4	$9654 < X < 10346$
4×10^4	$19511 < X < 20489$
8×10^4	$39308 < X < 40692$
10^6	$497555 < X < 502445$

Significance level $\alpha = 10^{-7}$	
Length of n	Accept region
2×10^4	$9623 < X < 10377$
4×10^4	$19467 < X < 20533$
8×10^4	$39246 < X < 40754$
10^6	$497335 < X < 502665$

3.1.3 포커 검정

포커 검정은 길이가 2만 비트인 표본수열을 길이가 4 비트인 블록으로 구분하여 전체 5000개의 블록 중 같은 값을 가지는 블록의 개수가 균등한지 확인하는 적합도 검정이다. 임의의 5000개의 블록 중 j 번째 블록을 c_j 그리고 c_j에서 $i \in \{0,...,15\}$ 값이 발생한 경우의 수를 $f[i] = |\{j : c_j = i\}|$ 로 정의하면, 한 블록에서 발생할 수 있는 기댓값은 5000/16이다. 이때 포커 검정의 적합도 검정 값 Y는

$$\begin{aligned} Y &= \sum_{i=0}^{15} (f[i] - (5000/16))^2 / (5000/16) \\ &= (16/5000)\left(\sum_{i=0}^{15} f[i]^2\right) - 5000 \end{aligned}$$

이다. 이 경우 한 블록에서 발생할 수 있는 경우의 수는 16이므로 하나의 경우에 대한 블록의 기댓값은 5000/16이다. 그리고 16가지의 경우에서 15가지의 경우의 수가 정해지면 나머지 한 가지의 경우는 자연스럽게 정해지기 때문에, 검정 통계량은 자유도가 15인 카이제곱분포를 따른다. 또한 AIS.31에 제시된 포커 검정의 유의수준 α는 10^{-6} 이므로 식 (3)을 이용해 통과 기준 $y \approx 56.4$의 값을 구할 수 있다.

포커 검정의 일반화된 통과 기준은 자유도 d 와 유의수준 α 에 영향을 받는다. 이때 d 와 α 를 수식 (3)에 대입하면 통과 기준을 일반화할 수 있다. 아래의 Table 7.은 자유도 d가 15인 경우에 유의수준에 따른 통과범위를 제시한 것이다.

일반적으로 카이제곱검정은 단측검정으로 이루어진다. 하지만, 포커 검정의 경우에는 양측검정을 사용하여 표본의 난수성을 검정하고 있다. 포커 검정에서 양측검정으로 바꾸어 검정을 하는 이유는 계산 값이 0에 가까울수록 이상적인 랜덤에 가깝다는 뜻이지만, 진난수발생기의 출력에서 계산 값이 0으로 나온다는 것은 진난수발생기에 조작의 가능성이 있다고 보고 이것을 탐지하고자 하는 것으로 보인다.

Table 7. Accept regions of poker test

Significance level	Y (one-side test)	Y
10^{-4}	$0 < Y < 44.2$	$2.00 < Y < 45.2$
10^{-5}	$0 < Y < 50.4$	$1.42 < Y < 51.4$
10^{-6}	$0 < Y < 56.4$	$1.02 < Y < 57.4$
10^{-7}	$0 < Y < 62.3$	$0.74 < Y < 63.2$

3.1.4 런 검정

런 검정[2,9]은 표본수열에서 길이가 l인 런(연속된 0 또는 1)의 발생횟수를 검정하는 것으로 표본수열에서 연속적으로 동일한 비트 값이 나오는 것을 조

사하기 위한 검정이다. 길이가 n인 랜덤한 표본수열에서 길이 l인 런이 발생하는 개수를 확률변수 X라 정의하고 i번째 비트에서 길이가 l인 런의 발생유무를 나타내는 확률변수를 X_i라 하면, X는

$$X = X_1 + X_2 + \ldots + X_{n-l} + X_{n-l+1}$$

로 표현할 수 있다. 이때 런이 발생하는 위치에 따라 1)양 끝에서 길이가 l인 런이 발생하는 경우, 2)중간에서 길이가 l인 런이 발생하는 경우로 나누어 생각할 수 있다. 추가적으로 1)의 경우에는 첫 비트가 런의 시작인 경우와 마지막 비트가 런의 마지막인 경우 두 가지로 나누어 볼 수 있다.

1)은 Fig.4.와 같이 l비트가 1(또는 0) 값을 가지고 $l+1$번째 비트가 0(또는 1)이 되는 경우이다. 이때 길이가 l인 런이 발생할 확률은 $2^{-(l+1)}$이다. 2)는 Fig.5.에 나타나있는 것처럼 런의 양쪽의 수는 런을 이루는 수와 달라야 하므로 이때 길이가 l인 런이 발생할 확률은 $2^{-(l+2)}$이다. 또한 1)이 발생하는 경우의 수는 2이고 2)가 발생할 수 있는 경우의 수는 $n-(l+1)$이다.

X_i는 i번째 비트에서 런의 발생유무의 결과를 가지므로 이항분포를 따른다. 한편 1)의 경우는 2)의 경우와 다른 분포를 가지지만, 충분히 작은 수이기 때문에 1)의 경우도 2)의 분포를 따른다고 가정한다. 또한 각 비트가 독립이면 블록도 독립성을 갖기 때문에 X_i는 Table 8.과 같은 분포를 따른다.

위 내용을 정리하면 길이 l인 런의 분포는 평균과 분산이 각각

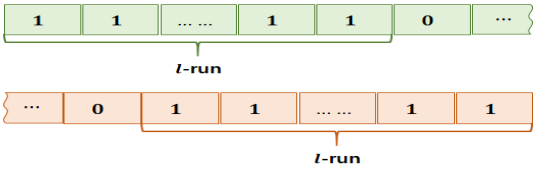

Fig. 4. Position of l-run is both ends

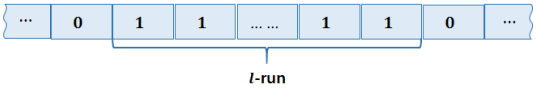

Fig. 5. Position of l-run is not both ends

Table 8. Distribution of X_i

X_i	0	1
$P(X_i)$	$1-2^{-(l+2)}$	$2^{-(l+2)}$

$$E[X] = \frac{n-l+3}{2^{l+2}}, \quad Var[X] = \frac{1}{2^{l+2}}\left(1-\frac{1}{2^{l+2}}\right)$$

인 정규분포로 근사한다.

런 검정의 일반화된 통과 기준은 표본수열의 길이 n과 유의수준 α에 영향을 받는다. 유의수준 α에 대응하는 z를 수식 (1)을 이용하여 구하고 평균값 $E[X]=\mu_X$, 분산 $Var[X]=\sigma_X^2$을 수식 (2)에 대입하여 통과 기준을 일반화한다. Table 9.는 유의수준 α가 10^{-6}일 때의 통과범위를 제시한 것이다.

Table 9. Accept regions of run test

The length of $n=2\times10^4$	
Length of run	Accept region
1	2272-2728
2	1083-1417
3	505-745
4	227-398
5	96-217
over 6	96-217

The length of $n=4\times10^4$	
Length of run	Accept region
1	4677-5323
2	2264-2736
3	1080-1420
4	504-746
5	227-398
over 6	227-398

The length of $n=8\times10^4$	
Length of run	Accept region
1	9543-10457
2	4666-5334
3	2260-2740
4	1079-1421
5	504-746
over 6	504-746

The length of $n=10^6$	
Length of run	Accept region
1	123383-126617
2	61317-63683
3	30400-32100
4	15019-16231
5	7382-8243
over 6	7382-8243

3.1.5 롱런 검정

롱런 검정은 표본수열에서 길이가 34이상인 런이 발생하는지 검정하는 것이다. 길이가 n 비트인 랜덤한 표본수열에서 k_l을 길이가 l인 런의 수라고 하자. 롱런 검정의 경우 표본수열 2만 비트에서 $k_{34}=0$ 인 경우를 찾는 것과 같다. 이때 길이가 l인 런이 발생하지 않는 경우의 수는 Fibonacci l-step Number[11]를 통해 구할 수 있다.

$$F_k^{(l)}=\sum_{i=1}^{l}F_{k-i}^{(l)},\ F_k^{(l)}=\begin{cases}0,\text{if } k\le 0\\ 1,\text{if } k=1,2\end{cases}$$

(Fibonacci l-Step Number)

Fibonacci l-Step Number를 이용하여 길이가 l인 런이 발생하지 않을 확률은

$$P(k_l=0)=\frac{F_{n+2}^{(l)}}{2^n}$$

으로 구할 수 있고, 유의수준 α는

$$P(k_l>0)\approx 2^{-l}(n-l)\approx\alpha \qquad (4)$$

과 같이 구할 수 있다[8]. 이때 길이가 34인 런이 발생하지 않을 확률은

$$P(k_{34}=0)=\frac{F_{20000+2}^{(34)}}{2^{20000}}$$

과 같고, 유의수준 α는

$$P(k_{34}>0)\approx 2^{-34}(20000-34)\approx 1.16\times 10^{-6}$$

으로 근사한다.

롱런 검정의 일반화된 통과 기준은 표본수열의 길이 n과 유의수준 α에 영향을 받는다. Table 10.은 수식 (4)를 이용하여 통과 기준을 일반화시킨 것이다.

Table 10. Accept regions of longrun test

$n=2\times10^4$	
Significance level	Length of l
10^{-4}	27
10^{-5}	30
10^{-6}	34
10^{-7}	37

$n=4\times10^4$	
Significance level	Length of l
10^{-4}	28
10^{-5}	31
10^{-6}	35
10^{-7}	38

$n=8\times10^4$	
Significance level	Length of l
10^{-4}	29
10^{-5}	32
10^{-6}	36
10^{-7}	39

$n=10^6$	
Significance level	Length of l
10^{-4}	33
10^{-5}	36
10^{-6}	40
10^{-7}	43

3.1.6 자기상관관계 검정

자기상관관계 검정은 표본수열 2만 비트에서 처음 1만 비트에 대해 위상이 5000 차이가 나는 비트, {i번째 비트$\oplus(i+5000)$번째 비트}를 이용하여 검정한다. {i번째 비트$\oplus(i+5000)$번째 비트}의 수열에서 1의 개수를 나타내는 확률변수를 Z_τ라 하면, Z_τ 역시 독립 반복 시행의 결과이므로 크기가 5000, 확률이 1/2인 이항분포를 따르게 된다. 그리고 5000은 충분히 큰 수이기 때문에 평균이 2500, 분산이 1250인 정규분포로 근사한다. 즉

$$Z_\tau\sim B\left(5000,\frac{1}{2}\right)\approx N(2500,1250)\ .$$

또한 자기상관관계 검정의 유의수준 α는 10^{-6} 이므로 수식 (1)을 이용하여 구한 $z\approx 4.89$, 평균 5000과 분산 1250을 수식 (2)에 대입하면 통과 기준 $2326<Z_\tau<2674$을 구할 수 있다.

자기상관관계 검정을 일반화하는 경우 {i번째 비트$\oplus(i+n/4)$번째 비트}가 새로운 비트가 된다. 새로운 비트 수열에서 1의 개수를 나타내는 확률변수를 X라 하면, X는 독립 반복 시행의 결과이므로 새로운 비트들은 크기가 $n/4$이고 발생확률이 1/2인 이항분포를 따르게 된다. 그리고 표본수열의 길이 $n/4$이 충분히 클 때, 평균과 분산이 각각

$$E[X]=\mu_X=\frac{n}{8},\quad Var[X]=\sigma_X^2=\frac{n}{16}$$

인 정규 분포로 근사한다. 즉

$$X\sim B\left(\frac{n}{4},\frac{1}{2}\right)\approx N\left(\frac{n}{8},\frac{n}{16}\right).$$

자기상관관계 검정의 일반화된 통과 기준은 표본수열의 길이 n과 유의수준 α에 영향을 받는다. 유의수준 α에 대응하는 z값, 평균과 분산을 수식 (2)에 대입하면 일반화된 통과 기준을 구할 수 있다. 일반화된 통과기준을 Table 11.에 제시한다.

Table 11. Accept regions of autocorrelation test

Significance level $\alpha=10^{-4}$	
Length of n	Accept region
2×10^4	$2362<X<2638$
4×10^4	$4805<X<5195$
8×10^4	$9724<X<10276$
10^6	$124027<X<125973$

Significance level $\alpha=10^{-5}$	
Length of n	Accept region
2×10^4	$2343<X<2657$
4×10^4	$4779<X<5221$
8×10^4	$9687<X<10313$
10^6	$123895<X<126105$

Significance level $\alpha=10^{-6}$	
Length of n	Accept region
2×10^4	$2326<X<2674$
4×10^4	$4755<X<5245$
8×10^4	$9654<X<10346$
10^6	$123777<X<126223$

Significance level $\alpha=10^{-7}$	
Length of n	Accept region
2×10^4	$2311<X<2689$
4×10^4	$4733<X<5267$
8×10^4	$9623<X<10377$
10^6	$123667<X<126333$

3.2 클래스 P2

디지털화된 잡음원이 클래스 P2에 속함을 보장해 주는 통계적 검정으로는 균일분포(T6), 다항분포(T7), 엔트로피(T8) 검정이 있다. Fig.6.은 진난수 발생기 내에서 클래스 P2 검정이 적용되는 지점을

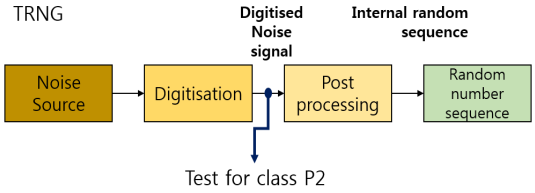

Fig. 6. Test for class P2

보여주고 있다. AIS.31 문서에서는 T6의 세부 검정법 2가지, T7의 세부 검정법 2가지에 T8을 포함한 5가지 검정법을 10만 비트 이상의 표본수열에 적용한 결과를 바탕으로 검정 통과 여부를 판정하고 있다. 여기에서는 클래스 P2의 검정법을 확률론적으로 분석하여 일반화된 검정 통과 범위를 제시하고자 한다.

3.2.1 균일분포 검정

균일분포 검정은 표본수열을 길이가 k 비트인 블록으로 나누어 보았을 때, 발생할 수 있는 모든 블록의 개수가 균등하게 분포해 있는지를 비율로 확인하는 검정이다. 균일분포 검정은 모노비트 검정과 같은 원리로 표본수열의 균등성을 검정하지만 차이점이 존재한다. 모노비트 검정이 1비트를 대상으로 표본수열 내의 1의 총 개수로 표본수열의 랜덤성을 검증하는 반면에, 균일분포 검정은 길이가 1 비트 이상인 블록에 대하여 각 블록값이 균일하게 분포하는지의 여부를 각각의 비율을 조사하여 검정한다는 점이 다르다.

표본수열을 길이가 k 비트인 n 개의 블록으로 나누었을 때, 한 블록에서 발생할 수 있는 모든 값에 대한 경우의 수는 2^k 개 이다. 그 중 하나의 경우가 발생한 것을 성공, 나머지를 실패로 본다면 표본 통계량은 크기가 n이고 성공확률이 $1/2^k$ 인 이항분포를 따른다. 성공 횟수를 확률변수 X라 하면, 표본수열 통계량의 분포는 평균과 분산이 각각

$$E[X]=\frac{n}{2^k},\quad Var[X]=\frac{n}{2^k}\left(1-\frac{1}{2^k}\right)$$

인 이항분포이고, 이는 중심극한정리에 의하여 정규분포로 근사한다. 균일분포 검정은 발생하는 모든 블록의 균등함을 비율로 보기 때문에 전체 블록의 개수 n으로 발생한 경우를 나누어야 한다. 이때 새로운 확률변수를 $Y=X/n$ 라 정의하면, Y는 평균과 분산을 각각

$$E[Y]=\mu_Y=\frac{1}{2^k},\ \ Var[Y]=\sigma_Y^2=\frac{1}{n2^k}\left(1-\frac{1}{2^k}\right)$$

으로 갖는 정규분포로 근사한다. 수식 (1)을 이용하여 유의수준 α에 대응하는 z를 구하면, 통과 기준은 수식 (2)와 유사한 방법으로 구할 수 있다. 즉

$$\mu_Y-z\,\sigma_Y\le Y\le\mu_Y+z\,\sigma_Y. \qquad (5)$$

또한 균일분포 검정은 k 비트에서 발생할 수 있는 모든 블록에 대한 통계량이 수식 (5)의 통과 기준을 만족할 때 균일분포 검정을 통과했다고 할 수 있다. Table 12.와 Table 13.에는 각각 k가 2, 4 일 때의 일반화된 통과 기준을 제시한다.

Table 12. Uniform distribution test for $k=2$

The length of $n=2\times10^4$	
Significance level	Accept region
10^{-4}	$0.2381<Y<0.2619$
10^{-5}	$0.2365<Y<0.2635$
10^{-6}	$0.2350<Y<0.2650$
10^{-7}	$0.2337<Y<0.2663$

The length of $n=4\times10^4$	
Significance level	Accept region
10^{-4}	$0.2416<Y<0.2584$
10^{-5}	$0.2404<Y<0.2596$
10^{-6}	$0.2394<Y<0.2606$
10^{-7}	$0.2385<Y<0.2615$

Table 13. Uniform distribution test for $k=4$

The length of $n=2\times10^4$	
Significance level	Accept region
10^{-4}	$0.05584<Y<0.06916$
10^{-5}	$0.05493<Y<0.07007$
10^{-6}	$0.05413<Y<0.07087$
10^{-7}	$0.05338<Y<0.07162$

The length of $n=4\times10^4$	
Significance level	Accept region
10^{-4}	$0.05779<Y<0.06721$
10^{-5}	$0.05715<Y<0.06785$
10^{-6}	$0.05658<Y<0.06842$
10^{-7}	$0.05605<Y<0.06895$

3.2.2 다항분포 검정

다항분포 검정은 일정 길이를 갖는 블록의 개수가 n인 표본수열을 h개 모았을 때, 표본수열의 블록에서 같은 값을 가지는 블록의 개수가 균등한지 확인하는 적합도 검정이다. Fig.7.에 나타난 것처럼 하나의 블록에서 발생할 수 있는 경우의 수는 s가지이다. 하지만, 실제 비트 단위로 구현이 되기 때문에 본 논문에서는 $s=2^x$ 꼴이라 가정하고 분석했음을 밝힌다.

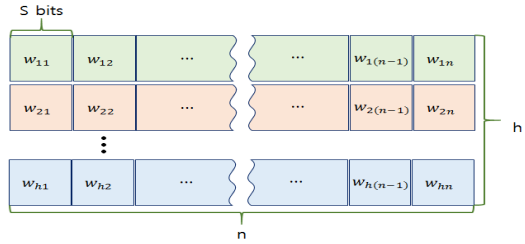

Fig. 7. Comparative test for multinomial

다항분포 검정의 i번째 표본수열에서 $t\in\{0,...,s-1\}$값이 발생한 경우의 수를 $f_i[t]$로 정의하면 $f_i[t]$는 $f_i[t]=|j:w_{ij}=t|$ 로 표현할 수 있다. 이 때 전체 표본수열에서 t값이 발생하는 상대도수는

$$p_t=(f_1[t]+...+f_h[t])/(hn)$$

이다. 이 경우 다항분포 검정 값을 확률변수 Y로 정의하면,

$$Y=\sum_{i=1,...,h}\sum_{t=0,...,s-1}(f_i[t]-np_t)^2/np_t$$

이다. Y는 전체 블록에서 h개의 부분 표본수열에서 t가 발생하는 상대도수의 합으로 검정하기 때문에, 적합도 검정의 자유도는 s와 h에 의존하며 $(s-1)(h-1)$이다.

다항분포 검정은 포커 검정과 같이 표본수열의 적합도를 검정하는 점에서 유사하다. 하지만 포커 검정의 경우 4비트에 대한 적합도 검정으로 단위 블록에서 발생할 수 있는 경우의 수가 16으로 고정되어 있는 반면, 다항분포 검정의 경우 한 블록에서 발생할 수 있는 경우의 수가 s개로 고정 되어있지 않다는 점에서 차이가 있다.

다항분포 검정의 일반화된 통과 기준은 자유도 d와 유의수준 α에 영향을 받는다. Table 14.는 수식 (3)을 이용하여, $s=2$일 때, $h=2,4$인 경우의 통과 기준을 나타낸 표이다.

Table 14. Comparative test for multinomial in case of $h=2,4$

$h=2$ (degree 1)	
Significance level	Y
10^{-4}	$Y<15.13$
10^{-5}	$Y<19.51$
10^{-6}	$Y<23.93$
10^{-7}	$Y<28.37$

$h=4$ (degree 3)	
Significance level	Y
10^{-4}	$Y<21.11$
10^{-5}	$Y<25.90$
10^{-6}	$Y<30.66$
10^{-7}	$Y<35.41$

3.2.3 엔트로피 검정

엔트로피 검정은 Maurer의 유니버설 검정법[12]을 향상시킨 검정법이다[13]. 이 검정법은 먼저 Fig.8.과 같이 표본수열을 길이가 L인 블록 $Q+K$개로 나눈다. 이 중 앞의 Q개는 초기화 부분으로 K개의 검정 부분의 블록과 같은지 비교하는 역할을 한다. 초기화 부분에 검정 블록과 동일한 블록이 있는지 비교하여 검정 블록과 가장 가까운 동일한 블록과의 위치차이를 통해 대상의 엔트로피를 추정한다.

표본이 이상적이라면 블록의 엔트로피는 L이 된다. 이때 $Q \geq 10\times 2^L$, $K \geq 1000\times 2^L$을 만족하면 평균과 분산이 각각 L, σ^2인 정규분포로 근사한다[13]. 여기서 σ는 참고문헌 [13]의 Table 1.을 통해 얻을 수 있다. 또한 엔트로피 검정은 그 결과가 7.976 초과인 경우 통과이다[2]. 이를 바탕으로 엔트로피 검정 분석을 통해 얻은 수식의 하한이 통과기준이 되는 것으로 분석할 수 있다. 이를 바탕으로 Table 15.는 $L=8$인 경우의 유의수준에 따른 엔트로피 검정 통과 기준을 나타낸 것이다.

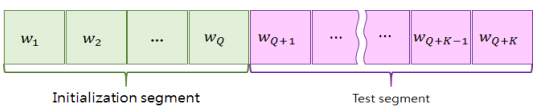

Fig. 8. Entropy test

Table 15. Accept boundary values of entropy test

L \ α	10^{-3}	10^{-4}	10^{-5}	10^{-6}	10^{-7}
8	7.9953	7.9945	7.9937	7.9931	7.9925

IV. 반복시행을 이용한 통과 기준

Ⅳ장에서는 반복시행과 신뢰구간(confidence interval) 개념을 사용하여 일반화된 AIS.31 통계적 검정을 반복적으로 시행할 수 있는 환경에서 필요로 하는 통과 기준을 제안한다. 이때 모비율 추정을 도구로 하여 반복시행 횟수 N과 유의수준 α에 따른 통과 기준을 제시한다. 모든 w_i가 독립 동일 분포를 따를 때, 길이가 2만 비트인 N개의 표본수열을 $w_1, w_2, ..., w_N \in \{0,1\}^{20000}$라 하자. 각 w_i는 유의수준 α를 기준으로 '표본이 랜덤하다', '표본이 랜덤하지 않다'로 나누어지기 때문에, 통과 확률을 $1-\alpha$, 실패 확률을 α로 볼 수 있다. 표본은 통과하거나 실패하는 두 가지 경우만 가지기 때문에, 전체 검정 표본은 크기가 N이고 확률이 $1-\alpha$인 이항분포를 따른다고 판단할 수 있다. 이에 확률변수 X를 검정을 통과한 w_i의 개수라 하고, 통과한 w_i의 비율을 확률변수 $Y=X/N$라 하면, 충분히 큰 N에 대하여 Y의 분포는 평균과 분산이 각각 $1-\alpha$, $\alpha(1-\alpha)/N$인 정규분포로 근사한다. 즉

$$Y \sim N\left(1-\alpha, \frac{\alpha(1-\alpha)}{N}\right).$$

검정 표본 N개의 난수성을 평가하기 위해서 신뢰구간 개념을 적용하면 아래의 수식 (6)를 얻는다. 이때 $\sigma=\sqrt{\alpha(1-\alpha)/N}$이고 $z_{\gamma/2}$는 수식 (1)의 $1-\gamma$에 대응하는 값이다.

$$(1-\alpha)-z_{\gamma/2}\,\sigma \leq Y \leq (1-\alpha)+z_{\gamma/2}\,\sigma \qquad (6)$$

Table 16.과 Table 17.은 유의수준 α를 가진 검정 표본을 N회 반복시행 했을 때 표본수열의 난수성을 판단하기 위한 통과 기준을 나타낸다. 표는 다음과 같이 해석할 수 있다. 신뢰도 95% 또는 99%로 Y를 추정했을 때 추정치에 N을 곱한 값인 전체 검정 표본에서 난수성 검정을 통과한 횟수가 기준 이상인 경우, 표본수열은 난수성을 가진다고 판단할 수 있다. 추가적으로 N값과 유의수준 α의 곱이 1보다 큰 경우, 즉 $N\times\alpha \geq 1$ 일 때 반복시행을 이용한 통과 기준이 의미를 가진다.

Table 16. Accept regions of iterative test when confidence level is 95%($z_{\gamma/2}=2$)

Significance level $\alpha = 10^{-3}$		
N	Interval of Y	Accept region
10^3	$0.9970010 < Y$	$998 \le X$
10^4	$0.9983678 < Y$	$9984 \le X$
10^5	$0.9988001 < Y$	$99881 \le X$
10^6	$0.9989367 < Y$	$998937 \le X$
10^7	$0.9989800 < Y$	$9989801 \le X$

Significance level $\alpha = 10^{-4}$		
N	Interval of Y	Accept region
10^3	$0.9992675 < Y$	$1000 \le X$
10^4	$0.9997000 < Y$	$9998 \le X$
10^5	$0.9998367 < Y$	$99984 \le X$
10^6	$0.9998800 < Y$	$999881 \le X$
10^7	$0.9998936 < Y$	$9998937 \le X$

Table 17. Accept regions of iterative test when confidence level is 99%($z_{\gamma/2}=3$)

Significance level $\alpha = 10^{-3}$		
N	Interval of Y	Accept region
10^3	$0.9960015 < Y$	$997 \le X$
10^4	$0.9980517 < Y$	$9981 \le X$
10^5	$0.9987001 < Y$	$99871 \le X$
10^6	$0.9989051 < Y$	$998906 \le X$
10^7	$0.9989700 < Y$	$9989701 \le X$

Significance level $\alpha = 10^{-4}$		
N	Interval of Y	Accept region
10^3	$0.9989513 < Y$	$999 \le X$
10^4	$0.9996000 < Y$	$9997 \le X$
10^5	$0.9998051 < Y$	$99981 \le X$
10^6	$0.9998700 < Y$	$999871 \le X$
10^7	$0.9998905 < Y$	$9998906 \le X$

Ⅳ장에서 제시한 반복시행을 이용한 통과 기준은 두 가지 경우에 사용될 것으로 기대된다. 먼저 잡음원 수집이 어려운 환경에서 2만 비트씩 간헐적으로 수집한 N개 표본 전체의 난수성을 검정하고자 하는 경우에 사용될 수 있다고 기대한다. 예를 들면, 잡음원 수집이 어려운 환경에서 수집한 표본 10만 비트에 대한 통과 기준은 수식 (5)에 $N=5$를 대입하여 구할 수 있다. 다음으로 유의수준 α를 변화함으로써 동일한 N개의 보안제품 내부의 난수발생기에서 출력한 표본수열 2만 비트를 수집하여 보안제품의 안전성을 비교하는 데 사용될 수 있다고 기대한다.

Ⅴ. 실험 및 결과

5.1 실험 목적

AIS.31에 대한 확률론적인 분석 결과를 바탕으로 본 논문에서 제시한 일반화된 검정 방법의 유효성을 입증하기 위하여 현재 상용화 되어 있는 난수발생기에 대한 실험을 실시하였다. 실험 대상으로는 IDQuantique SA[16]에서 출시한 제품인 양자난수발생기 Quantis와 비교적 널리 알려진 리눅스 난수발생기인 LRNG[17]를 선정하였다. 제조사에서는 Quantis를 진난수발생기로 주장하고 있으며, 최종 출력수열은 후처리 과정을 거친 이후의 것으로 보아야 한다. 그러므로 우리는 이에 대해서 클래스 P1 검정을 적용하기로 하였다. 또한, 클래스 P1을 일반화한 결과를 추가적으로 검정하기 위하여 LRNG의 중간 잡음원으로부터 추출한 수열과 최종 출력 수열을 구분하여 검정을 실시하였다.

한편, 클래스 P2의 검정 방법을 일반화하여 적용하는 방법의 경우 아직은 코드 구현을 위한 경험론적인 방법을 적용하기에 성숙되지 않은 면이 있고, 현실적으로는 완제품으로 출시된 진난수발생기의 중간 잡음원을 추출하는 기술적인 어려움이 존재하기 때문에 추후의 연구 과제로 남겨두기로 하였다.

5.2 실험 환경 및 방법

Quantis는 양자 물리적 잡음원을 후처리 행렬에 통과시키는 원리로 최종 난수를 발생시킨다. 실험에 사용한 Quantis는 보드형태로 컴퓨터에 장착하고 실행 소프트웨어를 설치한다. 이 소프트웨어를 통해 난수 2MB를 획득한다.

리눅스 난수발생기는 잡음원 수집 단계, 엔트로피 측정 및 저장 단계, 난수 출력 단계 세 단계를 통해 난수를 발생시킨다. 먼저 잡음원 수집 단계에서는 하드웨어 의존 잡음원인 user input, device information, disk I/O, interrupt, hardware RNG의 출력 데이터를 수집하는 단계이다. 두 번째 엔트로피 측정 및 저장 단계는 1단계에서 수집한 잡음원을 mixing 함수의 입력으로 하여 그 출력을 엔트로피 풀에 저장하는 단계이다. 마지막 난수 출력 단계는 엔트로피 풀에 저장된 잡음원을 SHA-1의

입력으로 하여 난수를 출력하는 단계이다. 본 실험에는 1단계 잡음원 수집 단계의 잡음원인 interrupt의 Cycle noise source 2MB와 최종 출력물인 LRNG_/dev /random 2MB를 실험 대상으로 하여 실험을 진행하였다.

검정 표본의 난수성을 측정하는 도구로는 독일 BSI에서 제공하는 JAVA 코드[12]를 영어로 번역하여 사용하였다.

- 실험 환경 : Intel(R) Core(TM) i7-4790K CPU @ 4.00 GHz 4.00 GHz, 16.0GB RAM
- 실험 대상 : Quantis source
  LRNG_Cycle noise source
  LRNG_/dev/random
- 표본수열의 길이 : 2만 비트, 4만 비트
- 유의수준 : 10^{-4}, 10^{-6}

본 논문 결과의 유효성을 검증하기 위해 유의수준과 표본수열의 길이를 변화시켜 실험을 한다. 먼저 표본수열의 길이가 2만 비트인 경우, BSI에서 제공한 JAVA 코드를 사용하여 유의수준 10^{-4}과 유의수준 10^{-6}에 대하여 실험 대상들의 클래스 P1 검정의 통과유무를 확인한다. 다음으로 표본수열의 길이가 4만 비트인 경우, 4만 비트의 유의수준 10^{-4}과 유의수준 10^{-6}에 대응하는 통과 기준을 JAVA 코드에 적용하여 실험 대상들의 클래스 P1 검정 통과유무를 확인하는 방법으로 진행한다.

5.3 실험 결과

5.3.1 표본수열의 길이 2만 비트

첫 번째 실험은 표본수열의 길이를 2만 비트로 설정했을 때, 유의수준에 따른 통과유무를 확인하는 실험이다. Fig.9.의 실험대상은 LRNG_Cycle source이다. LRNG_Cycle source는 유의수준 10^{-4}과 10^{-6} 모두 통과하지 못하였다. Fig.11.은 클래스 P1의 257번 검정 중 유의수준을 10^{-4}으로 강화시킨 일반화된 통과 기준의 의미 있는 부분을 캡쳐한 것이다. LRNG_Cycle source는 유의수준 10^{-6}에서는 포커 검정을 통과한 반면 유의수준을 10^{-4}으로 강화시킨 경우에는 포커 검정을 통과하지 못하였다. LRNG_Cycle source의 계산된 포커 검정의 값은 약 51.10이다. 포커 검정의 통과 기준이 유의수준이 10^{-6}인 경우 1.03 초과 57.3 미만이기 때문에 통과하였지만, 유의수준을 10^{-4}으로 강화시킨 경우 포커 검정의 통과 기준이 2.00 초과 45.2 미만으로 강화되었기 때문에 포커 검정을 통과하지 못하였다.

Fig.10., Fig.11.의 실험대상은 각각 LRNG source와 Quantis 소스다. 각 실험 대상은 유의수준 10^{-6}과 10^{-4}의 경우 모두 클래스 P1 검정을 통과하였다. 이는 AIS.31의 기준은 진난수발생기 작동 중에 완전붕괴를 검출해내는 온라인 검정에 대한 기준이고 Quantis 소스와 LRNG source는 난수발생기의 최종 출력물이기 때문에 온라인 검정에 대한 기준과 강화시킨 기준을 쉽게 통과한 것으로 보인다.

5.3.2 표본수열의 길이 4만 비트

두 번째 실험은 표본수열의 길이를 4만 비트로 설정했을 때, 유의수준에 따른 통과유무를 확인하는 실험이다. Fig.12.의 실험대상은 LRNG_Cycle source이다. LRNG_Cycle source는 유의수준 10^{-4}과 10^{-6} 모두 통과하지 못하였다. Fig.14.는 클래스 P1의 257번 검정 중 유의수준을 10^{-4}으로 강화시킨 일반화된 통과 기준이 의미를 가지는 부분을 캡쳐한 것이다. LRNG_Cycle source는 유의수준이 10^{-6}인 경우 모노비트 검정을 통과한 반면에 유의수준을 10^{-4}으로 강화시킨 경우에는 모노비트 검정을 통과하지 못하였다. LRNG_Cycle source의 계산된 모노비트 검정의 값은 19528이다. 표본수열의 길이가 4만 비트일 때 유의수준이 10^{-6}인 경우 모노비트 검정의 통과 기준이 19511 초과 20489 미만이기 때문에 통과하였지만, 유의수준을 10^{-4}으로 강화시킨 경우 모노비트 검정의 통과 기준이 19611 초과 20389 미만으로 강화되었기 때문에 모노비트 검정을 통과하지 못하였다.

Fig.13., Fig.14.의 실험대상은 각각 LRNG source와 Quantis 소스다. 각 실험대상은 유의수준 10^{-6}과 10^{-4}의 경우 모두 클래스 P1 검정을 통과하였다. 첫 번째 실험과 동일한 이유로 AIS.31은 진난수발생기 작동 중에 완전붕괴를 검출해내는 온라인 검정에 대한 기준이고 Quantis 소스와 LRNG source는 난수발생기의 최종 출력물이기 때문에 온라인 검정에 대한 기준과 강화시킨 기준을 쉽게 통과

한 것으로 보인다.

같은 실험대상에 대하여 유의수준을 달리하였을 때 표본수열의 난수성 검정 통과유무가 달라짐을 확인하였다. 이 실험을 통해 유의수준 변화에 따른 검정 통과의 여부로 난수성에 대한 우열을 평가할 수 있음을 확인하였고 이것은 Ⅲ장의 분석 결과가 유효함을 보여준다.

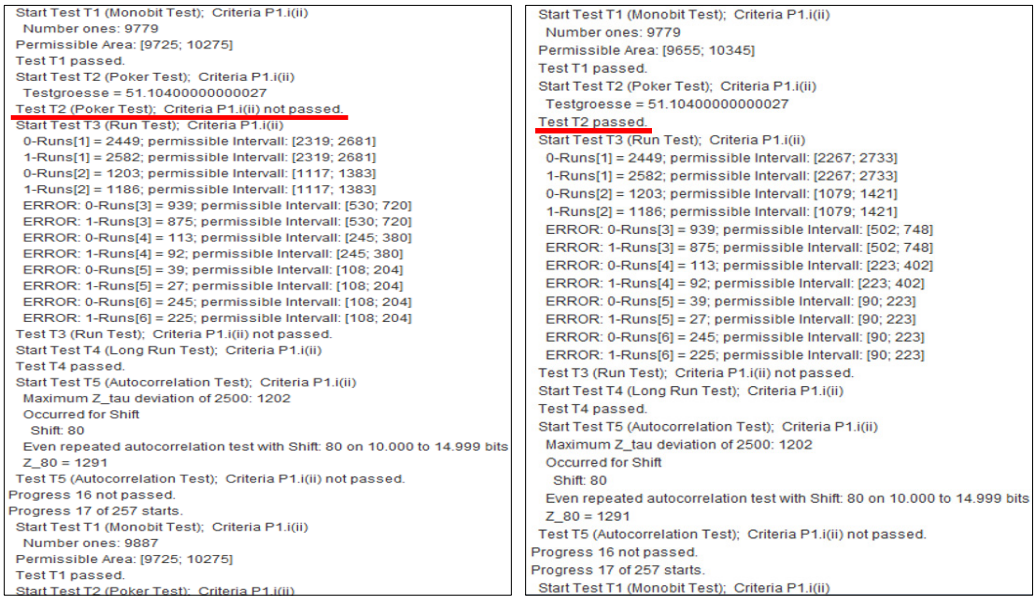

Fig. 9. For 20,000 bits sample sequence, apply AIS.31 criterion(right) to LRNG_Cycle source and 10^{-4} criterion(left) to LRNG_Cycle source

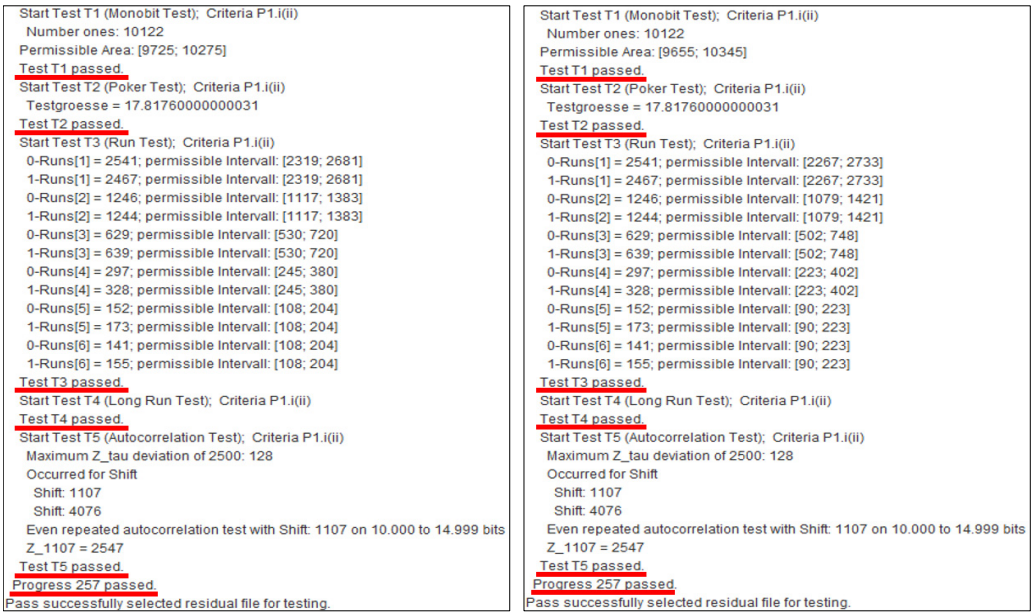

Fig. 10. For 20,000 bits sample sequence, apply AIS.31 criterion(right) to LRNG source and 10^{-4} criterion(left) to LRNG source

Fig. 11. For 20,000 bits sample sequence, apply AIS.31 criterion(right) to Quantis source and 10^{-4} criterion(left) to Quantis source

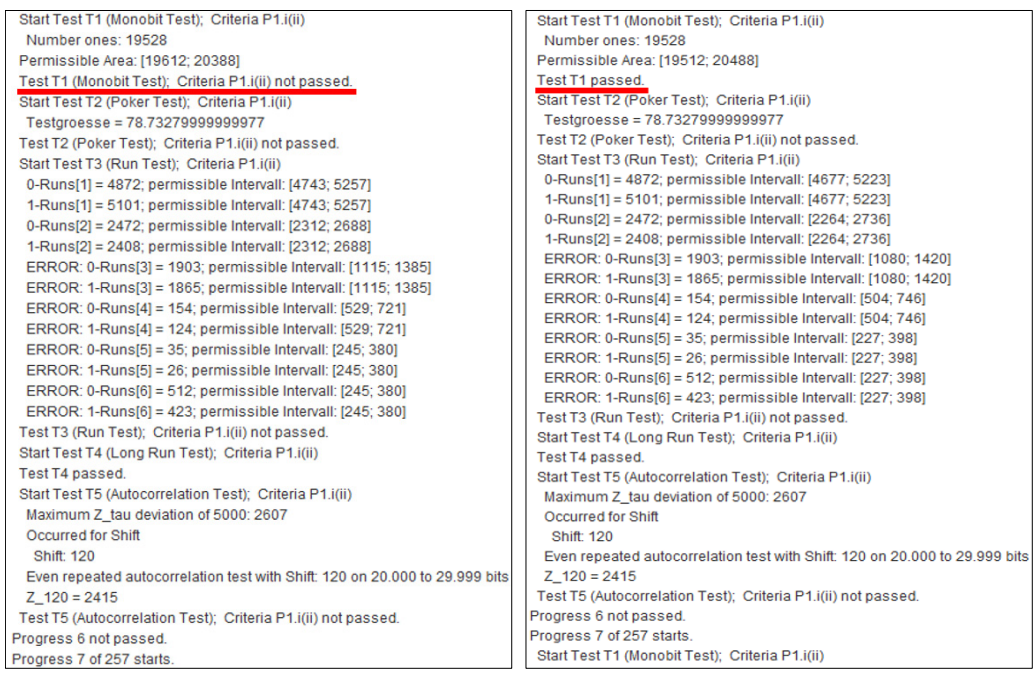

Fig. 12. For 40,000 bits sample sequence, compare results for LRNG_Cycle source when significance level 10^{-4}(left) and 10^{-6}(right)

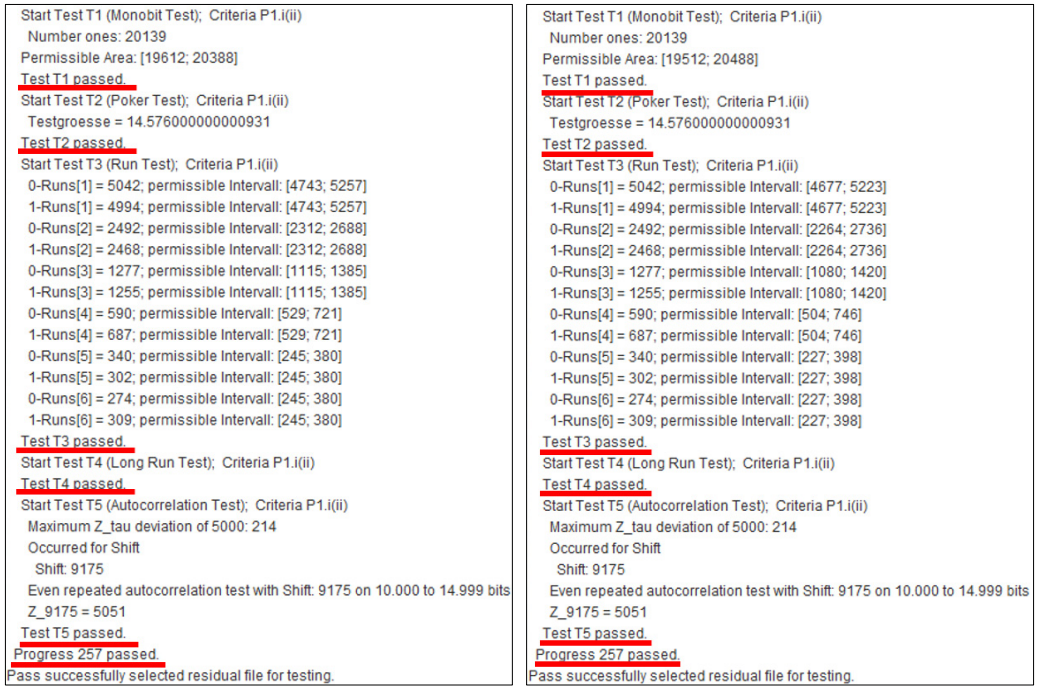

Fig. 13. For 40,000 bits sample sequence, compare results for LRNG source when significance level 10^{-4}(left) and 10^{-6}(right)

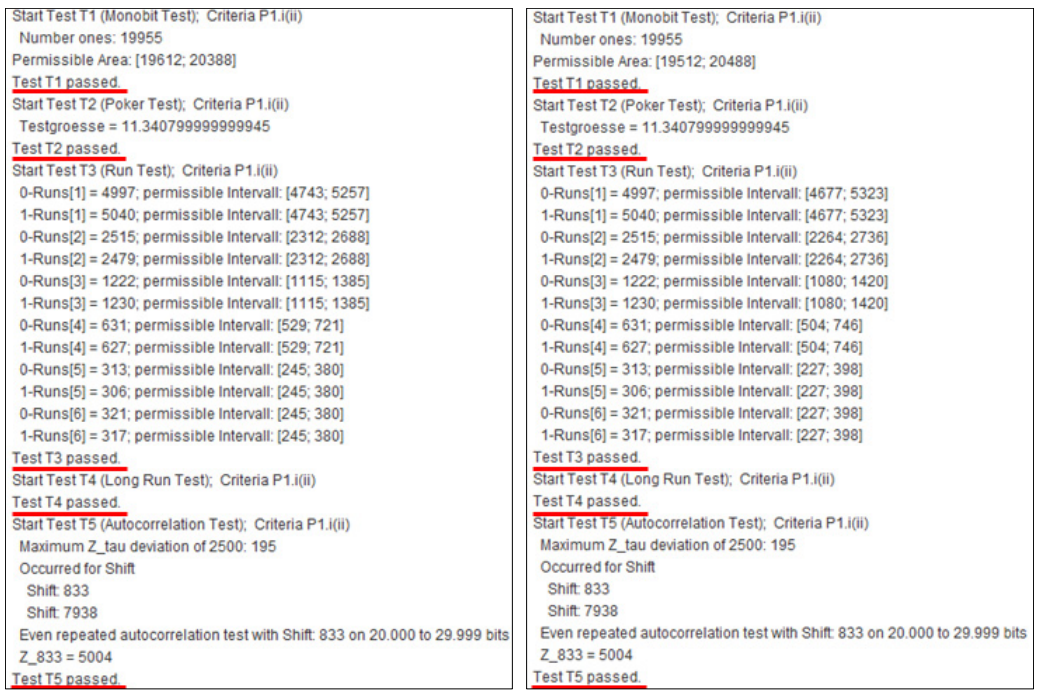

Fig. 14. For 40,000 bits sample sequence, compare results for Quantis source when significance level 10^{-4}(left) and 10^{-6}(right)

VI. 결 론

본 논문에서는 독일 BSI의 AIS.31 문서에 나타나 있는 통계적 검정 방법들을 확률론적 분석을 면밀히 분석하였다. 분석을 바탕으로 다음 세 가지 결과를 얻을 수 있었다. 첫째, 각 통계적 검정이 어떤 분포를 따르고 있는지 확인하였다. 둘째, 분석한 분포를 바탕으로 기존에 주어진 표본수열의 길이 n과 유의수준 α를 변화시켜 일반화된 통과 기준을 도출하였다. 마지막으로 신뢰구간 개념을 사용하여 일반화된 AIS.31 통계적 검정을 반복적으로 시행할 수 있는 환경에서 필요로 하는 통과 기준을 제안하였다.

본 연구의 결과는 대표적으로 다음의 두 가지 경우에 활용될 것으로 기대된다. 첫 번째로 기존의 방법은 표본수열의 길이 2만 비트로 고정되어 있었기 때문에 잡음원 수집에 관련된 다양한 환경에서의 적용하는데 어려움이 있었다. 반면, 본 연구에서 분석한 일반화된 AIS.31 통계적 검정은 표본수열의 길이와 유의수준을 일반화한 수식이다. 따라서 잡음원 수집이 어려운 환경부터 잡음원 수집이 용이한 환경에서 난수열을 평가하는 경우 본 연구의 결과가 합리적인 기준이 될 것으로 기대된다. 두 번째로 표본수열 2만 비트를 반복적으로 시행하는 방법을 응용함으로서 하나의 난수발생기의 난수성 평가뿐 만아니라, 다수의 난수발생기에서 출력한 표본수열에 대한 기준을 제안할 수 있었다. 이러한 특징으로 현장에서 서로 다른 다양한 종류의 보안제품의 안전성을 비교해야하는 경우에 본 연구가 활용될 수 있을 것으로 기대한다.

References

[1] Wolfgang Killmann and Werner Schindler, "A Proposal for : Functionally classes and evaluation methodology for true(physical) random number generators," AIS.31, Sep. 2001.

[2] Wolfgang Killmann and Werner Schindler, "Functionality Classes and Evaluation Methodology for Random Number Generators," AIS.20/AIS.31, Sep. 2011.

[3] Werner Schindler, "Functionality Classes and Evaluation Methodology for Deterministic Random Number Generators," AIS.20, Dec. 1999.

[4] Ronald H. Brown and James H. Burrows, "Security Requirements for cryptographic modules," FIPS 140-1, Jan. 1994.

[5] Donald L. Evans, Phillip J. Bond and Arden L. Bement, "Security Requirements for cryptographic modules," FIPS 140-2, May. 2001.

[6] Andrew Rukhin, et al. "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," NIST Special Publication 800-22 revision 1a, Apr. 2010.

[7] Elaine Barker and John Kelsey, "Recommendation for the Entropy Sources Used for Random Bit Generation," NIST Special Publication 800-90B, Aug. 2012.

[8] Thomas Risse, "Quality of Pseudo Random Numbers is the Quality of their Generators," 31st Int. Conf. Science in Practice, Oct. 2013.

[9] Jean Dickinson Gibbons and Subhabrata Chakraborti, Nonparametric Statistical Inference Fourth Edition, Marcel Dekker, pp 76-86, 2003.

[10] Fabio Pareschi, Riccardo Rovatti and Gianlca Setti, "On statistical Test for Randomness Included in the NIST SP800-22 Test Suite and Based on the Binomial Distribution," IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, vol. 7, no. 2, pp. 491-505, Apr. 2012.

[11] Eric Weisstein, Fibonacci k-step number, Available at http://mathworld.wolfram.com/Run.html.

[12] Alfred Menezes, Paul Van Oorschot and Scott Vanstone, "Handbook of APPLIED CRYPTOGRAPHY," Available at http://cacr.uwaterloo.ca/hac/. 2001.

[13] Jean-Sébastien Coron, "On the Security of Random Sources," PKC'99, LNCS 1560, pp. 29-42, 1999.

〔14〕 Referenzimplementierung der statistischen Tests/Reference implementation of the statistical tests, https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/ZertifizierungnachCCundITSEC/AnwendungshinweiseundInterpretationen/AIS/aiscc_node.html.
〔15〕 Sheldon Ross, A First Course in probability 9th Ed., PEARSON, Jan. 2009.
〔16〕 ID Quantique SA, Available at http://www.idquantique.com/random-number-generation/quantis-random-number-generator/.
〔17〕 Patrick Lacharme, Andrea Rock, Vincent Strubel and Marion Videau, "The Linux Pseudorandom Number Generator Revisited," HAL archives -ouvertes, Jun. 2014.

〈저자소개〉

박 호 중 (Hojoong Park) 학생회원
2015년 2월: 국민대학교 수학과 학사
2015년 3월~현재: 국민대학교 일반대학원 금융정보보안학과 석사과정
〈관심분야〉 암호이론, 정보보호 알고리즘 및 프로토콜, 난수성 분석

강 주 성 (Ju-Sung Kang) 종신회원
1989년 2월: 고려대학교 수학과 학사
1991년 2월: 고려대학교 일반대학원 수학과 석사
1996년 2월: 고려대학교 일반대학원 수학과 박사
1997년~2004년: 한국전자통신연구원 선임연구원/팀장
2001년~2002년, 2010년: 벨기에 루벤대학 COSIC 방문 연구원
2004년~현재: 국민대학교 수학과 교수
2013년~현재: 국민대학교 BK21+ 미래 금융정보보안 인력양성사업단 교수
〈관심분야〉 암호이론, 정보보안 프로토콜, 안전성 분석 및 평가

염 용 진 (Yongjin Yeom) 종신회원
1991년 2월: 서울대학교 수학과 학사
1994년 2월: 서울대학교 수학과 석사
1999년 2월: 서울대학교 수학과 박사
2000년 4월~2012년 2월: ETRI 부설연구소 책임연구원/팀장
2006년 12월~2007년 12월: Columbia 대학교 방문 연구원
2012년 3월~현재: 국민대학교 수학과 부교수
2013년~현재: 국민대학교 BK21+ 미래 금융정보보안 인력양성사업단 교수
〈관심분야〉 암호구현 및 분석, 보안시스템 평가