TTA Standard

정보통신단체표준(국문표준)

TTAx.xx-xx.xxxx/R1 제정일: 20xx년 xx월 xx일

소프트웨어 암호모듈에 사용되는 잡음원 시험평가 지침

Noise Source Testing Guidelines for Software Cryptographic Modules

TTA 한국정보통신기술협회
Telecommunications Technology Association

표준초안 검토 위원회	**응용보안 및 평가인증 프로젝트그룹(PG504)**
표준안 심의 위원회	**정보보호 기술위원회(TC5)**

	성명	소 속	직위	위원회 및 직위	표준번호
표준(과제) 제안	염용진	국민대학교	교수	WG5041 부의장	
	최희봉	NSR	책임연구원	WG5041 의장	
표준 초안 작성자	염용진	국민대학교	교수	WG5041 부의장	
	최희봉	NSR	책임연구원	WG5041 의장	
	서석충	NSR	연구원	-	
	주왕호	NSR	연구원	-	
	박호중	국민대학교	연구원	-	
	김예원	국민대학교	연구원	-	
사무국 담당	김재웅	TTA	단장	-	
	문서연	TTA	전임연구원	-	

본 표준 발간 이전에 접수된 지식재산권 확약서 정보는 본 표준의 '부록(지식재산권 확약서 정보)'에 명시하고 있으며, 이후 접수된 지식재산권 확약서는 TTA 웹사이트에서 확인할 수 있습니다.
본 표준과 관련하여 접수된 확약서 외의 지식재산권이 존재할 수 있습니다.

발행인 : 한국정보통신기술협회 회장
발행처 : 한국정보통신기술협회
13591, 경기도 성남시 분당구 분당로 47
Tel : 031-724-0114, Fax : 031-724-0109
발행일 : 2018.12

서 문

1 표준의 목적

이 표준에서는 소프트웨어 암호모듈에 활용되는 난수발생기의 잡음원에 대한 시험평가 절차 및 기준을 제시한다. 이 표준은 암호모듈 검증제도에 따른 시험평가기준 및 관련 TTA, ISO/IEC 표준들과 연계하여 안전한 난수발생기의 구현에 기여할 수 있도록 정량적 평가 방법 및 기준을 제공함으로써 개발업체와 시험기관에서 활용할 수 있도록 하고자 한다.

2 주요 내용 요약

암호모듈의 안전성을 보장받기 위해서는 암호키, 보안매개변수, 논스 등의 생성에 사용되는 난수가 암호학적 난수발생기로부터 안전하게 생성되어야 한다. 암호학적 난수발생기는 크게 엔트로피 수집 단계와 의사난수 생성 단계로 나눌 수 있으며, 이에 대한 평가방법으로는 의사난수 생성에 사용되는 결정론적 알고리즘의 구현 정확성을 검증하는 CAVP(Cryptographic Algorithm Validation Program)와 잡음원에 대한 안전성 평가방법인 통계적 난수성 검정과 엔트로피 테스트가 있다.
잡음원에 대한 통계적 난수성 검정으로는 미국 NIST의 SP 800-22와 독일 BSI의 AIS.31이 대표적으로 활용되고 있지만, 충분히 큰 데이터를 수집해야한다는 점과 잡음원의 분포는 예측할 수 없다는 점을 고려했을 때 통계적 난수성 검정만으로는 잡음원의 안전성을 검증하기에 어려움이 존재한다. 또한, 잡음원에 대한 엔트로피 테스트로는 미국 NIST의 SP 800-90B가 활용되고 있지만, NIST SP 800-90B 역시 충분히 큰 데이터를 수집해야하기 때문에 고속으로 생성되는 하드웨어 잡음원의 평가에 적합하다는 특징이 있다. 이와 같은 이유로 소프트웨어 암호모듈 위주인 국내 환경에 위의 두 가지 평가방법을 직접 적용하기에는 한계가 존재한다.
이에 이 표준에서는 소프트웨어 암호모듈 위주인 국내 환경을 고려하여 “소프트웨어 환경에서의 난수발생기 잡음원 엔트로피 검증 알고리즘”(TTAK.KO-12.0306/R1)을 인용 표준으로 하여, 인용 표준에 제시된 검증 알고리즘을 활용한 소프트웨어 암호모듈의 잡음원에 대한 시험평가 절차와 그 정량적인 기준을 제시한다. 이 표준에서는 잡음원 시험평가 절차, 시험평가 항목 및 기준과 소프트웨어 암호모듈에서 수집된 잡음원으로 암호학적 난수발생기의 씨드키를 생성하는 가이드를 제시한다.

3 인용 표준과의 비교

3.1 인용 표준과의 관련성

이 표준은 소프트웨어 환경에서의 잡음원 엔트로피 검증 알고리즘(TTAK.KO-12.0306/R1)을 기반으로 하여 소프트웨어 암호모듈에서 수집된 잡음원의 시

험평가 방법 및 정량적인 기준을 제시한다. 인용 표준에서는 소프트웨어 환경에서 수집한 잡음원의 시험평가로 사용 가능한 알고리즘을 제공한다. 인용 표준에서 제공하는 알고리즘으로는 통계적 난수성 테스트 5종(모노비트 검정, 포커 검정, 런 검정, 롱 런 검정, 자기 상관관계 검정), 잡음원 건전성 테스트 2종(반복 횟수 테스트, 적응성 비율 테스트), 확률론 및 정보이론 기반 엔트로피 측정 6종(최빈값 추정, 충돌 추정, 마코브 추정, 압축 추정, 엔트로피 테스트, 상호정보량 기반의 엔트로피 추정), 엔트로피 건전성 확인 방법 3종(바이트 상관관계 기반 엔트로피 측정, 비트/바이트 간 독립성 검정, 취약 패턴 검출 방법)이 있다. 이 표준에서는 인용 표준의 통계적 난수성 테스트 5종, 잡음원 건전성 테스트 2종, 확률론 및 정보이론 기반 엔트로피 측정 5종(최빈값 추정, 충돌 추정, 마코브 추정, 압축 추정, 엔트로피 테스트), 엔트로피 건전성 확인 방법 3종을 활용하여 소프트웨어 암호모듈의 운영환경에서 수집된 잡음원의 시험평가로 활용될 수 있는 정량적인 통과 기준을 제시한다.

3.2 인용 표준과 본 표준의 비교표

TTAK.xx-xx.xxxx	TTAK.KO-12.0306/R1	비고
6.1 통계적 특성 시험	5.1 통계적 난수성 테스트	TTAK.KO-12.0306/R1의 알고리즘을 인용하고 정량적인 통과 기준은 이 표준에서 설정함
6.2 건전성 테스트	5.2 잡음원 건전성 테스트	
6.3 엔트로피 측정	6 확률론 및 정보이론 기반 엔트로피 측정	
6.4 최종 점검	6 확률론 및 정보이론 기반 엔트로피 측정 7 엔트로피 건전성 확인 방법	

Preface

1 Purpose

The standard is to specify the testing guidelines and its criterion for noise sources generated from software cryptographic modules. It recommends that vendors and test laboratories use this standard with the relevant TTA, ISO/IEC standard documents and test requirement for CMVP(Cryptographic Module Validation Program) to securely implement random number generator.

2 Summary

To ensure the security of cryptographic modules, random numbers used to secret key, security parameters, nonce etc. shall be securely generated from cryptographic random number generator. The cryptographic random number generator is composed of two major step, which are collecting noise sources and generating pseudorandom numbers. The evaluation methods of the cryptographic random number generator are testing soundness of noise sources and CAVP(Cryptographic Algorithm Validation Program) for implementation conformance.

NIST SP 800-22 and BSI AIS.31 are usually used to verify the statistical randomness of the noise sources. However, there are some problems such that too many noise sources are required for the tests and the distributions of the noise sources are unknown. Thus, the tests have difficulty verifying the soundness of the noise sources. NIST SP 800-90B is used to estimate entropy of the noise sources, but it is appropriate to test the noise sources generated at high speed from hardware cryptographic modules due to be required too many noise sources. Therefore, it is also not suitable to directly apply these tests for noise sources generated from software cryptographic modules.

The standard is to propose the testing guidelines and its criterion using the algorithms which are cited in “Entropy Evaluation Algorithms for Noise Sources in Software Environments(TTAK.KO-12.0306/R1)” for considering our environments. The standard is to specify the testing guidelines, testing items and guide of generating the seed of cryptographic random number generator using the noise sources in software cryptographic modules.

3 Comparison with Reference Standard

3.1 Relationship to Reference Standards

The standard cites algorithms in reference standard, Entropy Evaluation Algorithms for Noise Sources in Software Environments(TTAK.KO-12.0306/R1). The reference standard provides testing algorithms for noise sources generated from the software environments. Reference standard is composed of five statistical randomness tests(Monobit test, Poker test, Run test, Long Run test and Autocorrelation test), two health tests(Repetition count test and Adaptive proportion test), six entropy measurements based on probability theory and information theory(the most common value estimation, Collision estimation, Markov estimation, Compression estimation, Entropy test, and Entropy estimation Based on Mutual Information), and three entropy health tests(Measurement of Entropy Based on Byte Correlation, Independent test for multi-byte/multi-bit, and Test for detecting the pattern). The standard is to propose the test criterion for noise sources generated from the software cryptographic modules by citing the five statistical randomness tests, the two health tests, the five entropy measurements based on probability theory and information theory(the most common value estimation, Collision estimation, Markov estimation, Compression estimation and Entropy test), and the three entropy health tests.

3.2 Comparison with Reference Standard

TTAK.xx-xx.xxxx	TTAK.KO-12.0306/R1	비고
6.1 Statistical Randomness Test	5.1 Statistical Randomness Test	The standard proposes the test criterion of the algorithms cited in TTAK.KO-12.0306/R1
6.2 Health Test	5.2 Health Test	
6.3 Entropy Estimation	6 Entropy Measurement Based on Probability Theory and Information Theory	
6.4 Sanity Check	6 Entropy Measurement Based on Probability Theory and Information Theory 7 Entropy Health test	

목 차

소프트웨어 암호모듈에 활용되는 잡음원 시험평가 지침 (Noise Source Testing Guidelines for Software Cryptographic Modules)

1 적용 범위

현대 암호에서 난수는 암호모듈이나 암호 시스템의 암호키, 보안매개변수, 논스, 암호학적 솔트 등의 암호학적 목적으로 사용된다. 암호학적 목적으로 사용되는 난수는 반드시 암호학적 난수발생기의 출력으로부터 구성되어야 하며, 이때 암호학적 난수발생기는 엔트로피 수집 단계에 사용되는 비결정론적 난수발생기(NDRBG, Non-Deterministic Random Bit Generator)와 의사난수 생성 단계에 사용되는 결정론적 난수발생기(DRBG, Deterministic Random Bit Generator)로 구성되어있다. 암호학적 난수발생기는 비결정론적 난수발생기의 출력을 결정론적 난수발생기의 입력인 씨드키로 사용하여 요청된 길이의 암호학적 난수를 출력하는 장치이다. 이때, 암호학적 난수발생기의 안전성은 잡음원의 예측 불가능성에 의존하기 때문에, 암호학적 난수발생기의 안전성 평가를 위해 잡음원으로부터 조합된 결정론적 난수발생기 입력의 안전성을 검증해야 한다. 이 안전성을 검증하는 대표적인 방법으로는 안전한 결정론적 난수발생기(의사난수 알고리즘)를 사용한다는 가정 하에서 진행되는 잡음원에 대한 엔트로피 테스트가 있다.
한편, 대부분의 국내 암호모듈은 소프트웨어 암호모듈이기 때문에, 이 표준에서는 국내 환경에 맞추어 소프트웨어 암호모듈에 사용되는 잡음원에 대한 시험평가 방법을 제시한다. 또한, 이 표준에서 제시하고 있는 시험평가 방법을 기반으로 결정론적 난수발생기의 입력인 씨드키를 안전하게 조합하는 가이드를 제시한다.
이 표준은 암호모듈 검증제도(KCMVP)에 따른 시험평가 기준 및 관련 표준들과 연계하여 소프트웨어 암호모듈에서 활용되는 잡음원의 엔트로피 시험평가 절차와 정량적 평가 기준을 제시한다. 이 표준이 제시한 기술은 암호모듈 개발자와 시험기관에서 암호모듈 안전성 검증 수행 시, 구현 정확성 검증인 CAVP와 함께 소프트웨어 암호모듈의 난수발생기 안전성 평가 방법으로 활용될 수 있다.

2 인용 표준

- 소프트웨어 환경에서의 잡음원 엔트로피 검증 알고리즘(TTAK.KO-12.0306/R1), 2018.

3 용어 정의

3.1 컨디셔닝 과정(Conditioning component)

수집된 잡음원의 편향성을 제거하여 엔트로피 비율을 조정하는 과정

3.2 암호모듈(Cryptographic Module)

적어도 한 개 이상의 검증대상 암호알고리즘을 탑재한 하드웨어와 소프트웨어 조합

3.3 결정론적 난수발생기(DRBG, Deterministic Random Bit Generator)

씨드키(Seed key)라고 부르는 초기 값으로부터 비트 열을 생성하는 알고리즘으로 구성되며, 동일한 씨드키 입력 시 동일한 비트열을 생성

3.4 엔트로피(Entropy)

폐쇄 시스템 내 무질서, 난수성, 변화성을 측정

3.5 엔트로피 비율(Entropy rate)

잡음원이 가진 엔트로피를 잡음원의 크기로 나눈 값으로 0과 1 사이로 표현됨

3.6 최소 엔트로피(Min-entropy)

예측 불가능성의 척도인 엔트로피 중 가장 작은 값으로 잡음원 샘플이 가질 수 있는 최악의 분포로부터 잡음원의 예측 불가능성을 측정한 값

3.7 잡음원(Noise Source)

난수발생기 씨드키를 구성하는데 사용되는 비결정론적인 데이터

3.8 비결정론적 난수발생기(NDRBG, Non-Deterministic Random Bit Generator)

예측 불가능한 물리적 소스에 의존하는 출력(비결정론적인 데이터)을 생성하는 요소
[출처] TTAK.KO-12.0235 운영체제별 잡음원 수집 및 응용 지침

3.9 개별화 문자열(Personalization string)

초기화 함수에서 작동 상태의 초기값을 결정할 때 사용되는 입력으로 난수 발생기마다 서로 다른 초기 작동 상태를 생성하도록 하기 위한 입력.
[출처] TTAK.KO-12.0189/R1 결정론적 난수발생기 -제1부- 블록암호 기반 난수발생기

3.10 유의 확률(P-value)

가설 검정에서 귀무가설(Null hypothesis(H_0): 난수는 랜덤하다)을 지지할 확률
유의 확률이 유의 수준보다 크다는 의미는 귀무가설을 지지할 확률이 높음을 의미함
즉, 테스트를 통과한 데이터는 설정한 유의 수준에 대해서 랜덤하다는 것을 의미함
[출처] TTAK.KO-12.0306 소프트웨어 환경에서의 난수발생기 잡음원 엔트로피 검증 알고리즘

3.11 난수발생기(RBG, Random Bit Generator)

통계적으로 독립되고 편중되지 않은 이진수열을 출력하는 장치 또는 알고리즘

3.12 샘플(Sample)

잡음원을 1회 출력한 데이터로, 이때 1회 출력되는 잡음원의 크기를 샘플 크기라 함

3.13 씨드키(Seed key)

난수발생기를 초기화하기 위해 사용하는 비밀값

3.14 샤논 엔트로피(Shannon Entropy)

예측 불가능성의 척도인 엔트로피 중 잡음원 샘플이 가지는 평균 정보량으로부터 잡음원의 예측 불가능성을 측정한 값

3.15 유의 수준(Significance level)

통계적 검정에서 귀무가설이 옳은데도 불구하고 틀린 것으로 판정하여 기각하는 확률
[출처] 국립국어원

3.16 벤더(Vendor)

암호모듈 검증을 신청하는 개체, 그룹 혹은 연합체

[출처(3.2, 3.4, 3.11, 3.13, 3.16)]
KS X ISO/IEC 19790. 정보기술 - 보안기술 - 암호모듈 보안 요구사항, 2015
[출처(3.1, 3.3, 3.5~3.7, 3.12)]
NIST SP 800-90B, Recommendation for the Entropy Sources Used for Random Bit Generation, 2018

4 약어 및 기호

4.1 약어

CAVP	Cryptographic Algorithm Validation Program
CMVP	Cryptographic Module Validation Program
DRBG	Deterministic Random Bit Generator
FIPS	The Federal Information Processing Standard
IID	Independent and Identically Distributed
KCMVP	Korean Cryptographic Module Validation Program
LSB	Least Significant Bit
MSB	Most Significant Bit
NDRBG	Non-Deterministic Random Bit Generator
Non-IID	Non-Independent and Identically Distributed
NIST	National Institute of Standards and Technology
SP	NIST Special Publication

4.2 기호

$\lfloor a \rfloor$	a 보다 작거나 같은 가장 큰 정수
$\ll$	왼쪽 비트 시프트(Shift)

5 잡음원 시험평가 절차

5.1 데이터 수집 방법

소프트웨어 암호모듈에서 수집되는 잡음원은 일정한 크기의 샘플 크기로 출력된다. 이때, 1 회 출력되는 샘플의 크기는 대부분 32 비트 이상이며, 잡음원마다 수집되는 샘플 크기는 다르다. 이 표준에서 제시하고 있는 잡음원 시험평가를 위해서는 적당한 간격으로 연속적으로 수집한 25만 개 이상의 샘플이 필요하며, 해당 샘플들은 전혀 가공되지 않은 상태이어야 한다. 즉, 수집하는 과정에서 잡음원의 통계적 특성에 영향을 주지 않도록 잡음원을 수집해야 함을 의미한다. 또한, 잡음원 시험평가를 위해 수집되는 잡음원은 그 샘플 크기에 따라 샘플 데이터를 구성하는 방법이 다르기 때문에, 샘플 크기가 8 비트 이하인 경우에 샘플 데이터를 수집하는 방법과 샘플 크기가 9 비트 이상인 경우에 샘플 데이터를 수집하는 방법을 각각 5.1.1 절과 5.1.2 절에 명시한다.

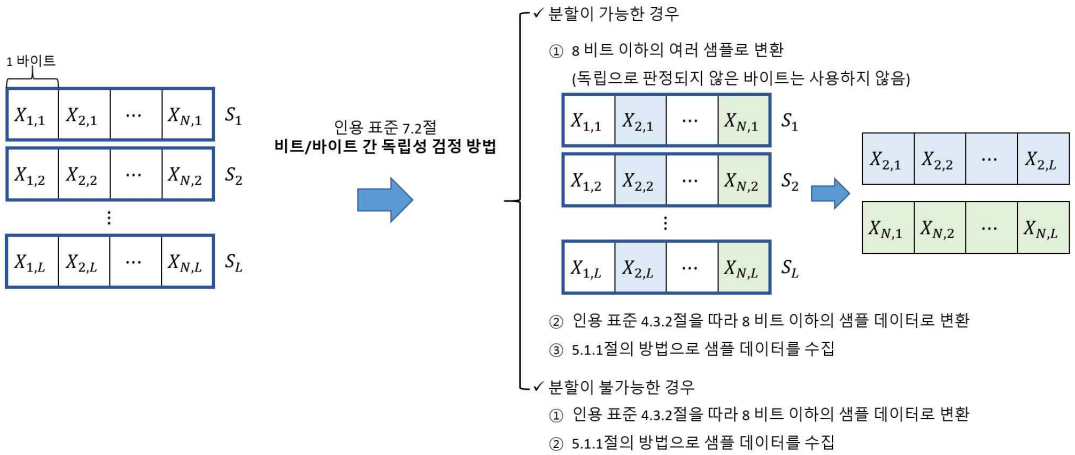
5.1.1 샘플 크기가 8 비트 이하인 경우

샘플 크기가 8 비트 이하인 경우에는 먼저 “소프트웨어 환경에서의 잡음원 엔트로피 검증 알고리즘(TTAK.KO-12.0306/R1)[1]”의 4.3.2 절에 근거하여 샘플 데이터를 구성하고, 그 값을 16 진수로 바이너리 파일에 저장한다. 이때 새롭게 구성된 샘플 데이터는 하위비트(LSB)부터 채워지며, 샘플 데이터 크기 이외의 공간은 0을 채워 저장한다. 즉, 샘플 데이터 크기가 i 비트인 경우에는 샘플 데이터 값이 0x00부터 $(1 \ll i)-1$ 로 표현되며, 그 값이 바이너리 파일로 저장된다. 예를 들어 샘플 데이터 크기가 4 비트인 경우에 샘플 데이터는 0x00부터 0x0f로 표현되어 파일에 저장된다. (그림 5-1)은 샘플 크기가 8 비트 이하인 경우의 새로운 샘플 데이터 구성, 샘플 데이터 크기에 따른 샘플 표현 범위 및 잡음원 수집 데이터의 저장 형식과 이를 바이너리 뷰어로 관측한 예시를 도식화 한 것이다. 이때 (그림 5-1)의 샘플 데이터 구성에서 파란색으로 표시된 부분이 샘플 비트이다.

(그림 5-1) 8 비트 이하의 샘플 구성 방법

5.1.2 샘플 크기가 9 비트 이상인 경우

샘플 크기가 9 비트 이상인 경우에는 (그림 5-2)와 같이 샘플 데이터 수집이 진행된다. 수집된 잡음원은 TTAK.KO-12.0306/R1의 7.2 절 “비트/바이트 간 독립성 검정 방법”을 이용하여 샘플을 독립적인 바이트로 분할이 가능한지 먼저 확인을 한다[1]. 이때 분할이 가능한 경우는 비트/바이트 간 독립성 검정에서 독립으로 판정된 바이트 위치를 의미한다. 분할이 가능한 위치들을 8 비트 이하의 여러 샘플로 변환한 후, TTAK.KO-12.0306/R1의 4.3.2 절에 근거하여 샘플 데이터를 구성한다[1]. 예를 들어, (그림 5-2)와 같이 샘플의 두 번째 바이트와 N 번째 바이트가 독립으로 판정되었다고 하자. 먼저, 독립으로 판정된 두 번째 바이트만 L 개 모은 샘플 열과 N번째 바이트만 L 개 모은 샘플 열을 구성하고, 나머지 바이트 열은 버린다. 다음으로 TTAK.KO-12.0306/R1의 4.3.2 절을 따라 각 샘플을 8 비트 이하의 샘플 데이터로 변환을 진행하고, 5.1.1 절 “샘플 크기가 8 비트 이하인 경우“의 방법으로 샘플 데이터를 수집한다[1].
반면, 분할이 불가능한 경우(비트/바이트 간 독립성 검정 방법에서 독립으로 판정되지 않은 경우)에는 TTAK.KO-12.0306/R1의 4.3.2 절을 따라 8 비트 이하의 샘플 데이터로 변환을 진행하고[1], 5.1.1절 “샘플 크기가 8 비트 이하인 경우”의 방법으로 샘플 데이터를 수집한다.



(그림 5-2) 샘플 크기가 9 비트 이상인 경우 샘플 데이터 수집 방법

잡음원의 시험평가를 위한 잡음원 수집 방법을 정리하면 벤더(Vendor)는 다음 조건을 만족하도록 샘플 데이터를 수집해야 한다.

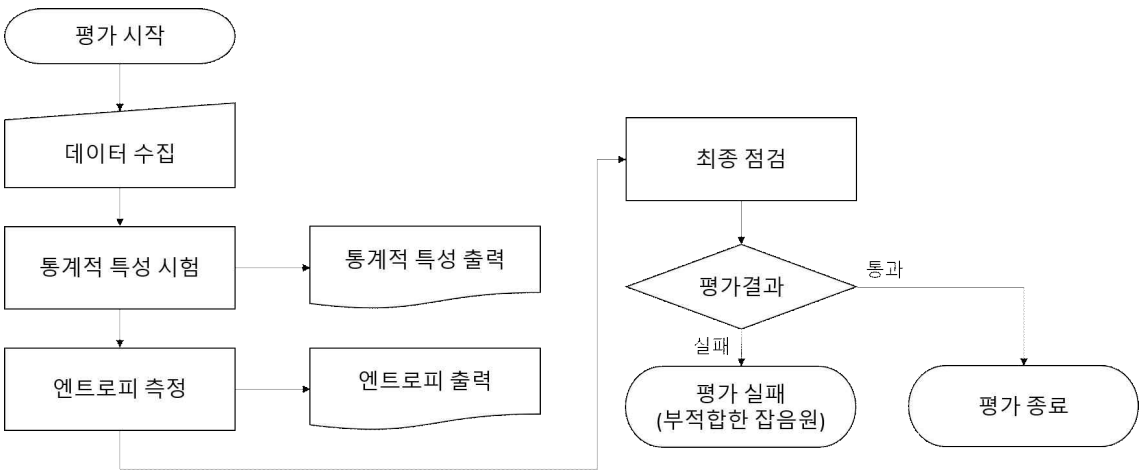
- 벤더(Vendor)는 잡음원의 통계적 특성이 변하지 않도록 전혀 가공되지 않은 25만 개 이상의 샘플을 연속적으로 수집해야 한다.
- 벤더(Vendor)는 잡음원 시험평가 진행을 위해 5.1.1 절, 5.1.2 절에 근거하여 잡음원 샘플 데이터를 구성해야한다.
- 벤더(Vendor)는 엔트로피 입력을 구성하는 잡음원 목록, 잡음원으로부터 엔트로피 입력까지 구성 단계 등 잡음원 사용에 대한 문서를 작성 및 제출하여야 한다.

5.2 시험평가 절차

잡음원의 엔트로피 시험은 “5.1 절 데이터 수집 방법”으로 수집된 샘플 데이터를 대상으로 진행된다. 잡음원의 엔트로피 시험은 통계적 특성 시험, 엔트로피 측정, 최종 점검의 세 단계로 구성되어있으며 (그림 5-3)과 같은 절차로 진행된다.

통계적 특성 평가의 목적은 잡음원의 통계적 특성을 파악하여, 반복 수집 가능한 잡음원과 아닌 잡음원을 분류하는 데에 목적이 있다. 이때, 반복 수집 가능한 잡음원은 씨드키 생성 단계에서 해당 잡음원의 출력을 여러 번 사용할 때, 잡음원이 가진 엔트로피를 독립적으로 인정하며, 단일 수집 잡음원은 씨드키 생성 단계에서 해당 잡음원이 가진 엔트로피를 한 번만 인정한다. 엔트로피 측정은 잡음원이 가진 최소 엔트로피를 측정하는 단계로 최빈값 추정, 충돌 추정, 마코브 추정, 압축 추정을 이용하여 잡음원의 최소 엔트로피를 측정한다. 최종 점검(Sanity Check)에서는 샤논(Shannon) 엔트로피 측정, 바이트 상관관계 기반 엔트로피, 취약 패턴 검출 방법을 이용하여 잡음원이 가진 취약성을 다시 한 번 확인하는 단계이다. 이때, 최종 점검은 샤논(Shannon) 엔트로피가 이론적으로 최소 엔트로피보다 항상 크거나 같다는 사실과, IID인 잡음원에 한정해서 두 바이트 간 상관관계 기반 엔트로피는 측정된 엔트로피의 두 배보다 작거나 같다는 관계와 잡음원의 취약 패턴 검출의 원리를 이용하여 잡음원의 통계적 이상 유·무를 최종적으로 확인한다.

한편, 최종 점검에서 최초로 실패한 잡음원에 대해서는 다음 두 가지 방법을 진행하여 잡음원의 엔트로피를 측정하도록 권장한다. 첫째, 샘플 데이터 변환에서 잡음원의 가장 많이 변화가 있는 비트를 정밀하게 선택하지 못한 경우일 수 있으므로, TTAK.KO-12.0306/R1의 4.3.2 절에 근거하여 수집된 잡음원의 샘플 데이터 크기를 기존보다 축소하여 잡음원 시험평가를 다시 진행한다. 둘째, 수집 간격을 늘이는 등 잡음원 수집 단계에서 변화를 주어 잡음원을 재수집한 후, 다시 잡음원 시험평가를 진행한다. 이때, 두 번째 시험평가의 최종 점검에서도 탈락한 잡음원의 경우, 부적합한 잡음원으로 판정하고 씨드키 생성 시 잡음원의 엔트로피를 씨드키의 엔트로피 계산에서 제외하고, 개별화 문자열(Personalization string)과 같이 보안성을 강화하기 위한 목적으로 결정론적 난수 발생기의 입력에 조합하여 씨드키를 생성한다[2].



(그림 5-3) 잡음원 시험평가 절차

6 시험평가 항목 및 기준

6.1 통계적 특성 시험

통계적 특성 시험(Statistical Randomness Test)은 반복 수집 가능한 잡음원을 판정하기 위한 절차로 <표 6-1>의 5 가지 시험 항목을 사용한다. 통계적 특성 시험에 사용되는 5 가지 시험 항목은 “소프트웨어 환경에서의 잡음원 엔트로피 검증 알고리즘(TTAK.KO-12.0306/R1)”의 5.1 절에 정의된 모노비트 검정, 포커 검정, 런 검정, 롱 런 검정, 자기 상관관계 검정이다[1,3,4]. 통계적 특성 시험을 진행하기 위해서는 TTAK.KO-12.0306/R1의 4.3.1 절에 근거하여 샘플 단위로 수집된 샘플 데이터를 비트열로 변환하여[1], 2만 비트 단위의 블록 k 개로 분할하는 절차가 먼저 진행되어야 한다.

<표 6-1> 통계적 특성 시험

	시험 항목
1	모노비트(Monobit) 검정
2	포커(Poker) 검정
3	런(Run) 검정
4	롱 런(Long run) 검정
5	자기 상관관계(Autocorrelation) 검정

통계적 특성 시험은 변환된 비트열을 대상으로 단위시험과 종합판정으로 나누어 진행되며, 종합판정을 통과한 잡음원에 대해서만 반복 수집 가능한 잡음원으로 판정한다. 여기에서 단위시험이란 분할한 2만 비트의 블록(단위 블록) 하나에 5 가지의 시험 항목을 적용하는 것을 의미하며, 단위 블록에 대한 테스트 결과가 이 표준에서 설정한 유의 수준 10^{-4} 보다 큰 경우에 단위시험을 통과했다고 판정한다. 한편, 종합판정은 k 개의 단위시험을 통과한 개수의 적절성을 판정하는 과정으로, 유의 수준 10^{-2} 과 신뢰구간의 하한을 이용하여 종합판정의 통과 기준(C)을 계산한다. 이때, 종합판정의 통과 기준(C)은 (수식 6-1)로 계산된다.

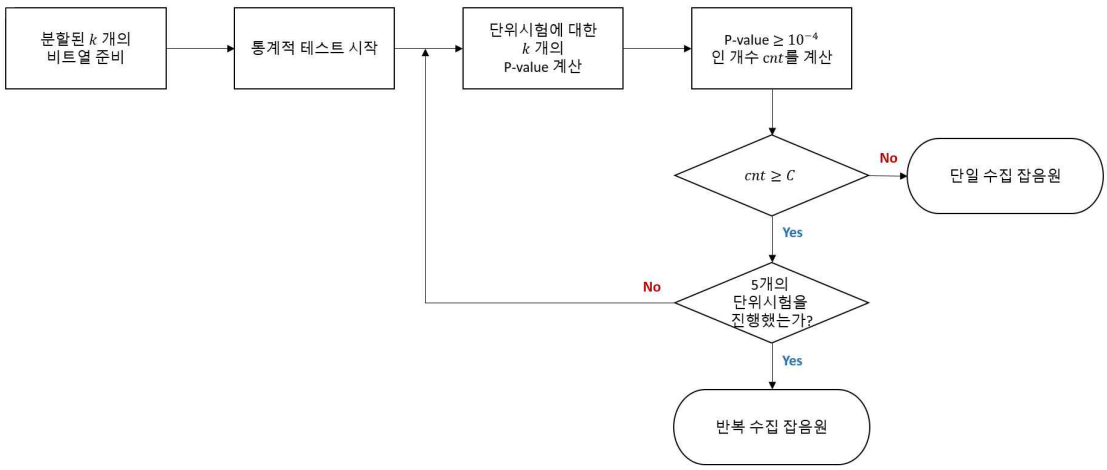
$$C \geq \left\lfloor k\times(1-10^{-4}) - 2.576\times\sqrt{\frac{10^{-4}\times(1-10^{-4})}{k}} \right\rfloor \qquad \text{(수식 6-1)}$$

이 표준에서는 2만 비트의 블록의 수 k 가 100 이상이 되도록 권고하며, <표 6-2>은 블록의 수 k 에 따른 종합판정 통과 기준(C)에 대한 예시이다.

<표 6-2> 블록의 수에 따른 종합판정 통과 기준

블록의 수(k)	통과 기준(C)
100	99
200	199
500	499
1,000	999
5,000	4,997
10,000	9,996

통계적 특성 시험은 (그림 6-1)과 같은 절차로 수행된다.



(그림 6-1) 통계적 특성 시험 흐름도

① 5.1절의 방법으로 수집된 25만 개 이상의 샘플 데이터를 연속적인 비트열로 구성한다. 비트열의 구성 방식은 TTAK.KO-12.0306/R1의 4.3.1 절을 따른다.
② 각 블록에 대한 단위시험을 수행하여 P-value를 얻는다.
③ P-value가 0.0001 보다 크면 통과 아니면 실패로 간주한다.
④ 5 개의 단위시험을 모두 통과한 경우, 즉, 종합판정을 통과한 경우에만 반복 수집이 가능한 잡음원으로 판정을 한다. 만일, 하나 이상의 시험을 통과하지 못하는 경우 단일 수집 잡음원으로 판정한다.

6.2 엔트로피 측정

소프트웨어 암호모듈에 사용되는 잡음원은 IID(Independent and Identically Distributed)의 특성을 만족하지 않는 Non-IID 데이터가 대부분이기 때문에, 잡음원의 최소 엔트로피

(Min-entropy) 값은 샘플 크기보다 작은 값을 가지는 것이 일반적이다. 또한 소프트웨어 암호모듈에서는 많은 잡음원을 수집하는 것이 어렵기 때문에, 잡음원의 최소 엔트로피 측정은 비교적 적은 데이터로 수행 가능한 방법인 TTAK.KO-12.0306/R1의 6.1절에 정의된 최빈값 추정, 충돌 추정, 마코브 추정, 압축 추정의 4가지 방법을 이용한다[1, 5]. 이때, 잡음원의 최소 엔트로피는 4가지 측정결과 중 가장 낮은 값으로 판정한다.

<표 6-3> 최소 엔트로피 측정 방법

	엔트로피 측정 방법
1	최빈값(The most common value) 추정
2	충돌(Collision) 추정
3	마코브(Markov) 추정
4	압축(Compression) 추정

한편, TTAK.KO-12.0306/R1의 마코브 추정에서 측정 가능한 최대 샘플 크기가 6비트이기 때문에, 샘플 데이터 크기가 8비트에 대한 엔트로피를 제공할 수 없다. 이에 이 표준에서는 다음의 두 가지 방법을 통해 가장 작은 값을 8비트 샘플 데이터에 대한 마코브 추정의 엔트로피로 판정한다.

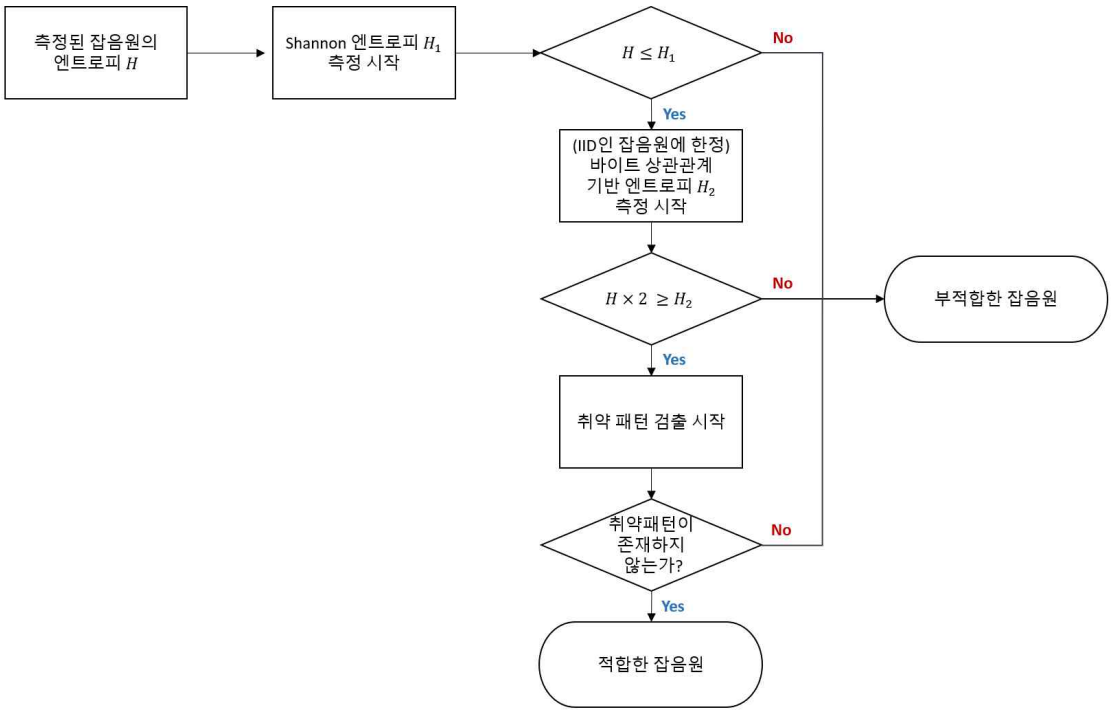
1) 하위 6비트 당 엔트로피 ÷ 6 × 8
2) 상위 4비트 당 엔트로피 + 하위 4비트 당 엔트로피

6.3 최종 점검

최종 점검(Sanity Check)은 소프트웨어 암호모듈에서 수집한 잡음원의 취약성을 확인하는 목적으로, TTAK.KO-12.0306/R1의 6.2절에 정의된 샤논(Shannon) 엔트로피 측정과 7절에 정의된 바이트 상관관계 기반 엔트로피 측정, 취약 패턴 검출 방법을 이용한다[1]. 이때 최종 점검의 판정은 (그림 6-2)와 같이 진행된다.

<표 6-4> 최종 점검(Sanity check)

	시험 항목
1	샤논(Shannon) 엔트로피 측정
2	바이트 상관관계 기반 엔트로피
3	취약 패턴 검출 방법



(그림 6-2) 최종 점검 흐름도

최종 점검에서 부적합한 잡음원으로 판정되는 경우는 다음의 3 가지가 있다.

① 6.4 절에서 측정된 엔트로피(H)가 샤논(Shannon) 엔트로피(H_1)보다 큰 경우
② IID인 잡음원에 한정하여, 측정된 엔트로피의 2 배($2 \times H$)가 두 바이트 간 상관관계 기반 엔트로피(H_2)보다 큰 경우
③ 취약 패턴이 검출된 경우

위 세 가지 방법을 최종 점검으로 사용하는 이유는 첫째, 최소 엔트로피는 샤논(Shannon) 엔트로피보다 작거나 같음이 증명되어 있고, 둘째, IID인 잡음원에 한정해서, 두 바이트 상관관계 기반 엔트로피는 최소 엔트로피의 2 배 이상이 되어야한다는 관계가 존재하고, 셋째, 통계적 특성 시험에서 검출하지 못한 잡음원의 취약성을 확인하기 위함이다.
한편, 최종 점검에서 처음 탈락한 잡음원의 경우 제안하는 두 가지 방법을 이용하여 잡음원 시험평가를 다시 진행한다. 첫째, TTAK.KO-12.0306/R1의 4.3.2 절에 근거하여 수집된 잡음원의 샘플 크기를 기존보다 축소하여 다시 잡음원 시험평가를 진행한다. 예를 들어, 샘플 크기가 8 비트인 잡음원이 최종 점검에서 탈락한 경우, 5.1 절에서 진행한 샘플 데이터 변환이 잡음원에서 가장 많이 변화가 있는 비트를 정밀하게 선택하지 못했기 때문에, TTAK.KO-12.0306/R1의 4.3.2 절의 방법을 이용하여 샘플 데이터 크기를 4 비트로 축소한 후에 다시 잡음원의 시험평가를 진행한다. 둘째, 수집 간격을 늘이는 등의 변화를 주어 잡음원 재수집한 후, 다시 잡음원 시험평가를 진행한다. 이때, 두 경우 모두 최종 점검을 통과한 경우에만 적합한 잡음원으로 판정을 하여 사용하고, 그렇지 않은 경우에는 부적합한 잡음원으로 판정한다. 한편, 부적합한 잡음원으로 판정된 잡음원은 측정

된 잡음원의 엔트로피를 씨드키의 엔트로피 계산에서 제외하지만, 씨드키 생성 단계에서 개별화 문자열(Personalization string)과 같이 보안성을 강화하기 위한 목적으로 결정론적 난수발생기의 입력에 조합하여 사용한다[2].

※ 최종 점검 단계에서 추가적인 시험평가가 요구되는 경우, 6.4 절 최종 점검과 별도로 6.3 절 엔트로피 측정에서 얻어진 최소 엔트로피를 입력으로 하여 또 다른 최종 점검으로서 NIST SP 800-90B의 재시작 테스트를 수행할 수 있다[5]. 재시작 테스트는 비결정론적 난수발생기를 1,000번 재시작하고 재시작마다 1,000 바이트를 수집한 비트열에 대하여 수행된다. 재시작 시 수집된 비트열끼리 상호 연관성이 있으면, 비결정론적 난수발생기는 엔트로피를 보장받지 못할 수 있다.

7 결정론적 난수발생기 입력 조합 방법

소프트웨어 암호모듈 내부에서 결정론적 난수발생기의 입력인 씨드키는 모듈 내에서 수집한 잡음원과 수집된 잡음원의 엔트로피 비율을 조정하는 컨디셔닝 과정을 통해서 만들어진다. 결정론적 난수발생기 입력 조합에서 컨디셔닝 과정이 필요한 이유는 일반적으로 소프트웨어 암호모듈에서 수집된 잡음원은 충분한 난수성을 가지지 않기 때문에, 수집된 잡음원을 씨드키로 직접 사용하는 것은 안전성 관점에서 적합하지 않다. 이러한 이유로 잡음원의 엔트로피 비율을 조정하는 컨디셔닝 과정을 적용하여 씨드키의 난수성을 확보하는 과정이 진행되어야 한다.
7 장 결정론적 난수발생기 입력 조합 방법에서는 6 장의 통계적 특성 시험을 통과한 잡음원과 컨디셔닝 과정을 이용하여 결정론적 난수발생기의 입력을 조합하는 방법을 제시한다. 또한, 안전한 씨드키 생성을 위해 난수발생기 내 잡음원 건전성 테스트를 소개하고, 벤더(Vendor)가 이를 구현하는데 사용할 수 있는 알고리즘, 건전성 테스트의 유의 수준 범위, 건전성 테스트의 구현 방안 등을 제시한다.
한편, 이 표준에서는 결정론적 난수발생기 입력 조합 방법에서 잡음원의 건전성 테스트를 사용 환경에 따른 선택사항으로 두었지만, 안전한 씨드키 생성을 위해 벤더(Vendor)에게 난수발생기 내의 건전성 테스트 구현을 권장한다.

7.1 컨디셔닝 과정

컨디셔닝 과정(Conditioning component)은 수집한 잡음원의 편향성을 제거하여 컨디셔닝 과정으로 출력된 잡음원의 엔트로피 비율을 조정하는 과정이다. 이 표준에서는 NIST SP 800-90B의 3.2.3 절을 참조하여 컨디셔닝 과정을 작성하였으며, 결정론적 난수발생기의 입력 조합에 사용 가능한 컨디셔닝 과정 알고리즘을 <표 7-1>에 제시한다[5].

<표 7-1> 컨디셔닝 과정에 사용 가능한 알고리즘

컨디셔닝 과정 알고리즘	특징
Hash Function	• 정의 : FIPS 180나 FIPS 202에 명시된 해시함수 • nw : 해시함수의 출력 비트 길이 • n_{out} : 해시함수의 출력 비트 길이
HMAC	• 정의 : FIPS 180 혹은 FIPS 202에 명시된 해시함수를 FIPS 198의 해시함수에 적용한 HMAC • nw : 해시함수의 출력 비트 길이 • n_{out} : 해시함수의 출력 비트 길이
CMAC	• 정의 : NIST SP 800-38B에 명시된 CMAC • nw : 128(AES의 블록 비트 길이) • n_{out} : 128(AES의 블록 비트 길이)
CBC-MAC	• 정의 : NIST SP 800-90B에 명시된 CBC-MAC • nw : 128(AES의 블록 비트 길이) • n_{out} : 128(AES의 블록 비트 길이)
Hash_df	• 정의 : NIST SP 800-90A에 명시된 Hash_df • nw : 해시함수의 출력 비트 길이 • n_{out} : 해시함수의 출력 비트 길이
Block_df	• 정의 : NIST SP 800-90A에 명시된 Block_df • nw : AES의 키 비트 길이 • n_{out} : AES의 키 비트 길이

이때, <표 7-1>에서 nw는 컨디셔닝 과정 알고리즘 내부의 요소에 대한 변수를 의미하며 n_{out}은 컨디셔닝 과정 알고리즘의 출력 비트 길이를 의미한다.
수집된 잡음원을 <표 7-1>에 제시된 컨디셔닝 과정 알고리즘을 이용하여 처리하였을 때, 컨디셔닝 과정 후의 엔트로피는 아래의 (수식 7-1)로 계산된다.

$$h_{out} = OutputEntropy(n_{in}, n_{out}, nw, h_{in}) \quad \text{(수식 7-1)}$$

여기에서 n_{in}은 컨디셔닝 과정 알고리즘에 입력되는 잡음원의 비트 길이, h_{in}은 컨디셔닝 과정 알고리즘에 입력되는 엔트로피 크기, h_{out}은 컨디셔닝 후의 엔트로피 크기를 의미하며, $OutputEntropy$는 다음의 과정을 통해 h_{out} 을 출력한다.

1. $P_{high} = 2^{-h_{in}}$, $P_{low} = \frac{1-P_{high}}{2^{n_{in}}-1}$로 정의한다.

2. 다음을 통해 n을 계산한다. $n = \min(n_{out}, nw)$
3. $\psi = 2^{n_{in}-n} P_{low} + P_{high}$를 계산한다.
4. $U = 2^{n_{in}-n} + \sqrt{2n(2^{n_{in}-n})\ln(2)}$ 을 계산한다.
5. $\omega = U \times P_{low}$으로부터 ω를 계산한다.
6. $h_{out} = -\log_2(\max(\psi, \omega))$으로부터 h_{out}을 계산한다.

예) 샘플 당 엔트로피가 2 비트인 32 비트 샘플 단위로 출력되는 잡음원 256 개 샘플에 컨디셔닝 과정을 적용한 경우[6]

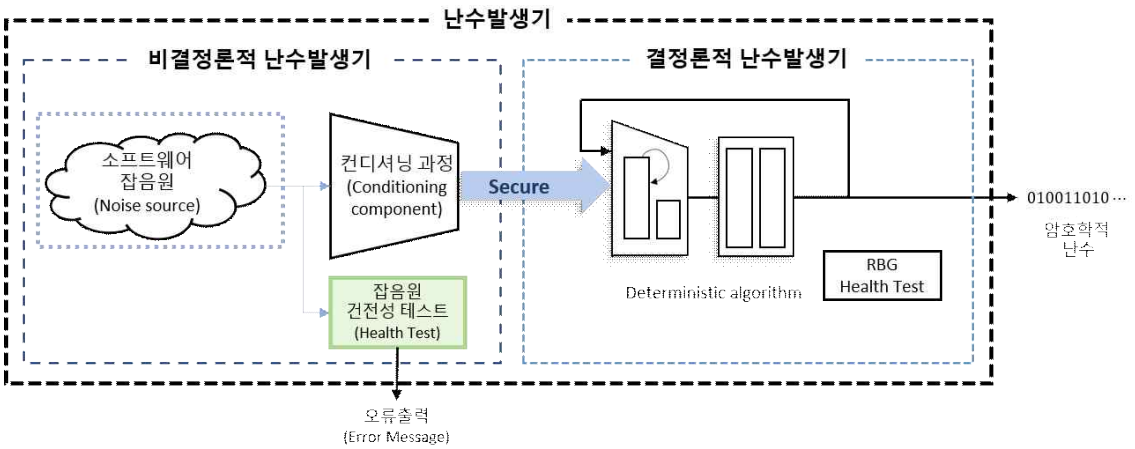
- 컨디셔닝 과정 알고리즘으로 FIPS 180의 SHA-256을 사용.
- SHA-256의 출력 비트 길이는 256 비트이므로 n_{out}와 nw는 256.
- 컨디셔닝 과정 알고리즘의 입력 길이 n_{in}은 32 비트 × 256 샘플인 $n_{in} = 8192$.
- $h_{out} = Output\ Entropy(8192, 256, 256, 512)$을 계산하면 $h_{out} = 256$.

7.2 건전성 테스트

잡음원의 건전성 테스트(Health test)는 난수발생기 내부에서 구현되어 실시간으로 잡음원을 모니터링하는 역할을 한다. 건전성 테스트는 잡음원의 통계적 문제점을 확인하는 과정이라기보다는, 장비의 노화 등으로 수집된 잡음원이 더 이상 정상 동작하지 않는 경우를 탐지하는 방법이다. 이때, 건전성 테스트에 사용되는 유의 수준은 $2^{-40} \sim 2^{-20}$ 범위에서 결정한다[5]. 건전성 테스트의 출력은 성공/실패의 2 가지이며, 건전성 테스트를 실패한 경우 잡음원을 더 이상 사용하지 않도록 한다.
잡음원 시험평가 지침에서 사용하는 건전성 테스트는 <표 7-2>에 제시되어 있으며, TTAK.KO-12.0306/R1의 5.2 절에 정의된 반복 횟수(Repetition count) 테스트와 적응성 비율(Adaptive proportion) 테스트이다[1].

<표 7-2> 건전성 테스트

	시험 항목
1	반복 횟수(Repetition count) 테스트
2	적응성 비율(Adaptive proportion) 테스트



(그림 7-1) 소프트웨어 암호모듈 내 난수발생기의 잡음원 건전성 테스트

잡음원의 건전성 테스트는 난수발생기 내부에서 (그림 7-1)에 작성된 것과 같이 컨디셔닝 과정 전의 잡음원을 대상으로 테스트가 진행된다. 벤더(Vendor)가 씨드키 생성과정에서 잡음원의 건전성 테스트를 적용하는 방법으로는 암호모듈 내에서 엔트로피가 수집될 때 마다 건전성 테스트를 진행하고, 건전성 테스트가 끝난 다음에는 건전성 테스트에 사용된 메모리를 모두 0으로 만드는 제로화를 적용하는 방법이 있다. 만약, 현재 수집되는 잡음원이 건전성 테스트에서 실패한 경우에는, 잡음원을 더 이상 엔트로피 소스로써 사용하면 안 된다. 한편, 이 표준에서는 결정론적 난수발생기 입력 조합 방법에서 건전성 테스트를 선택사항으로 두었지만, 안전한 씨드키 생성을 위해 난수발생기 내의 건전성 테스트 구현을 권장한다.

부 록 Ⅰ

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

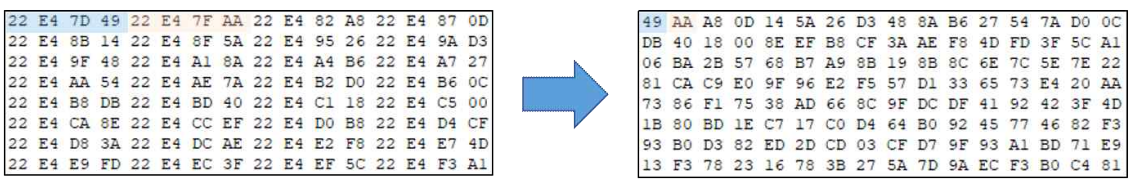
시험평가 적용사례

소프트웨어 암호모듈에서 수집 가능한 잡음원은 암호모듈 내에서 사용하는 운영체제에 따라 윈도우(Windows), 리눅스(Linux), 안드로이드(Android), 아이폰 운영체제(iOS) 잡음원 등으로 분류된다[7]. 운영체제 잡음원은 잡음원을 수집하는 시간 간격에 따라 잡음원의 특성이 달라지기 때문에, 운영체제 잡음원을 수집하는 간격은 잡음원 특성을 결정하는 중요한 요소이다[6]. 부록 Ⅰ에서는 실험적으로 분석된 잡음원인 윈도우 운영체제의 GetTickCount를 이용하여 시험평가 적용사례를 작성한다[5]. 잡음원 시험평가는 데이터 수집, 통계적 특성 시험, 엔트로피 측정, 최종 점검 순으로 진행된다.

Ⅰ.1 데이터 수집

데이터 수집 단계에서는 잡음원 수집과 수집된 잡음원을 시험평가에 적합하도록 변환하는 작업이 진행된다. 만약, 수집된 잡음원의 샘플 크기가 9 비트 이상인 경우에는 인용 표준의 7.2 절 “비트/바이트 간 독립성 검정 방법”을 이용하여 샘플을 독립적인 바이트로 분할 가능한지 확인한다. 바이트로 분할된 샘플은 인용 표준 4.3.2 절을 따라 8 비트 이하의 샘플로 변환하고, 5.1.1 절 “샘플 크기가 8 비트 이하인 경우”의 방법으로 데이터를 수집한다. GetTickCount는 다음의 과정으로 수집하였다.

- 윈도우 운영체제에서 GetTickCount를 0.5 초~1.5 초 사이의 랜덤한 간격으로 25만 샘플을 수집한다.
- GetTickCount의 샘플 크기는 32 비트이기 때문에[6], 인용 표준의 7.2 절 “비트/바이트 간 독립성 검정 방법”을 이용하여 샘플을 독립적인 바이트로 분할이 가능한지 확인한다.
- GetTickCount는 “비트/바이트 간 독립성 검정 방법”에서 종속으로 판정되었기 때문에, 인용 표준 4.3.2 절을 따라 8 비트의 샘플 데이터로 변환하고, 5.1.1 절 “샘플 크기가 8 비트 이하인 경우”의 방법으로 샘플 데이터를 수집한다.



(그림 Ⅰ.1-1) 5.1.1 절의 방법으로 수집한 GetTickCount

Ⅰ.2 통계적 특성 시험

통계적 특성 시험은 반복 수집이 가능한 잡음원인지 판정하는 단계이다. 통계적 특성 시험을 진행하기 위해 먼저, 인용 표준 4.3.1 절에 근거하여 수집한 샘플 데이터를 비트열로 변환하고, 이를 2만 비트 단위의 블록 k개로 분할한다. 통계적 특성 시험은 2만 비트 블록단위로 진행되는 단위시험과 단위시험을 통과한 횟수의 적절성을 판정하는 종합판정으로 구성되어 있다. 이때 종합판정까지 통과한 잡음원을 반복 수집 가능한 잡음원으로 판정한다. GetTickCount에 대한 통계적 특성 시험 결과는 다음과 같다.

- 수집한 GetTickCount의 샘플 크기는 8 비트이기 때문에 인용 표준 4.3.1 절에 근거하여 비트열로 변환하면, 2만 비트 단위의 블록 100 개로 분할된다.
- 수집한 GetTickCount의 통계적 특성 시험 결과는 100 개의 블록에서 단위시험을 모두 통과하여 통과 기준인 99 개를 넘어 종합판정을 통과하였기 때문에, 수집한 GetTickCount는 반복 수집이 가능한 잡음원으로 판정한다.

Ⅰ.3 엔트로피 측정

엔트로피 측정은 최빈값 추정, 충돌 추정, 마코브 추정, 압축 추정으로 측정된 엔트로피 중 최솟값을 잡음원의 엔트로피로 결정하는 단계이다. GetTickCount에 대한 엔트로피 측정 결과는 다음과 같다.

- 수집한 GetTickCount의 샘플 데이터 크기는 8 비트이기 때문에 마코브 추정은 1) 상위 4 비트 당 엔트로피와 + 하위 4 비트 당 엔트로피와 2) 하위 6 비트 당 엔트로피 ÷ 6 × 8에서 작은 값으로 추정한다.
- GetTickCount의 엔트로피 측정 결과는 아래와 같으며, 이때 최소인 7.0418을 GetTickCount의 엔트로피로 판정한다.
  - 최빈값 추정 : 7.7799
  - 충돌 추정 : 8.0000
  - 마코브 추정 : 7.0418
  - 압축 추정 : 8.0000

Ⅰ.4 최종 점검

최종 점검은 샤논(Shannon) 엔트로피, 바이트 상관관계 엔트로피, 취약 패턴 검출 방법을 이용하여 잡음원의 취약성을 확인하는 단계이다. 최종점검은 엔트로피 측정 단계에서 결정된 잡음원의 최소 엔트로피를 이용하여 진행된다. 최종 점검에서 탈락하는 경우는 샤논(Shannon) 엔트로피보다 측정된 최소 엔트로피가 큰 경우, IID인 잡음원에 한정하여 측정된 엔트로피의 2배가 바이트 상관관계 기반 엔트로피보다 큰 경우, 취약 패턴이 검출된 경우로 부적합한 잡음원으로 판정한다. 이때, 최종 점검에서 최초로 탈락한 경우에

는 잡음원 수집 단계부터 재시험이 진행되며, 재시험에서 탈락한 경우에는 씨드키를 생성할 때 엔트로피 계산에서 제외한 후 난수발생기의 입력에 조합하여 사용한다. 수집한 GetTickCount의 최종 점검 결과는 다음과 같다.

- GetTickCount는 IID인 잡음원이 아니기 때문에, 샤논 엔트로피와 취약 패턴 검출 알고리즘을 이용하여 최종 점검을 진행한다.
- 수집한 GetTickCount의 측정된 엔트로피는 7.0418이며, GetTickCount의 최종 점검 결과는 아래와 같이 통과하였기 때문에, 수집한 GetTickCount는 반복 수집이 가능하며 7.0418 비트의 엔트로피를 갖는 적합한 잡음원으로 판정한다.

  - 샤논(Shannon) 엔트로피 : 8.0000 > 7.0418
  - 바이트 상관관계 : -
  - 취약 패턴 검출 : 패턴이 없음

부 록 II-1

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

지식재산권 확약서 정보

II-1.1 지식재산권 확약서(1) : 해당 사항 없음

- 발명의 명칭
- 권리자의 성명
- 등록(출원) 번호
- 등록(출원) 연월일
- 실시조건
- 확약서 접수일

II-1.2 지식재산권 확약서(2) : 해당 사항 없음

- 발명의 명칭
- 권리자의 성명
- 등록(출원) 번호
- 등록(출원) 연월일
- 실시조건
- 확약서 접수일

부 록 II-2

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

시험인증 관련 사항

II-2.1 시험인증 대상 여부 : 해당 사항 없음

II-2.2 시험표준 제정 현황 : 해당 사항 없음

부 록 II-3

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

본 표준의 연계(family) 표준

II-3.1 TTAK.KO-12.0306/R1

인용 표준에서 제시하는 소프트웨어 환경에서의 난수발생기 잡음원 엔트로피 검증 알고리즘을 인용하여, 이 표준에서는 소프트웨어 암호모듈에서 수집된 잡음원에 대한 시험평가 절차와 그 정량적인 기준을 제시함

부 록 II-4

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

참고 문헌

[1] 소프트웨어 환경에서의 잡음원 엔트로피 검증 알고리즘, TTAS,KO-12.0306/R1, 2018.6.

[2] E. Barker and J. Kelsey, “Recommendation for Random Number Generation Using Deterministic Random Bit Generators”, NIST Special Publication 800-90A Revision 1, 2015.6.

[3] W. Killmann and W. Schindler, “A Proposal for : Functionality Classes and evaluation methodology for true(physical) random number generators”, BSI AIS.31, September, 2001.

[4] 박호중, 강주성, 염용진, “진난수발생기용 난수성 검정 방법 AIS.31에 대한 확률론적 분석 및 보안성 평가 적용 방법”, 한국정보보호학회논문지, 2016.2.

[5] M.S Turan, et al., “Recommendation for the Entropy Sources Used for Random Bit Generation”, NIST Special Publication 800-90B, January, 2018.

[6] 김예원, 염용진, “윈도우 운영체제의 시간 종속 잡음원에 대한 엔트로피 평가 방법 연구”, 한국정보보호학회논문지, 2018.8.

[7] 운영체제별 잡음원 수집 및 응용 지침, TTAS.KO-12.0235/R1, 2017.6.

[8] ISO, “Information technology — Security techniques - Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408”, ISO/IEC DIS 20543, 2018.

[9] KS X ISO/IEC 19790, 정보기술 — 보안기술 — 암호모듈 보안 요구사항, 2015.8.

※ 상기 기재된 참고 문헌의 발간일이 기재된 경우, 해당 표준(문서)의 해당 버전에 대해서만 유효하며, 연도를 표시하지 않은 경우에는 해당 표준(권고)의 최신 버전을 따름

부 록 II-5

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

영문표준 해설서

- 해당 사항 없음

부 록 II-6

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

표준의 이력

판수	채택일	표준번호	내용	담당 위원회
제1판	2018.12.xx	제정 TTAx.xx-xx.xxxx	소프트웨어 암호모듈에 활용되는 잡음원 시험평가 지침	PG504