논문 21-46-07-15 The Journal of Korean Institute of Communications and Information Sciences '21-07 Vol.46 No.07
https://doi.org/10.7840/kics.2021.46.7.1208

암호학적 난수발생기 잡음원의 분포 변화 탐지법

박 호 중◆, 권 수 진*, 염 용 진**, 강 주 성°

Methods to Detect Distribution Change for Noise Sources in Cryptographically Secure Random Number Generators

Hojoong Park◆, Sujin Kwon*, Yongjin Yeom**, Ju-Sung Kang°

요 약

암호학적으로 안전한 난수는 암호키, 보안프로토콜의 각종 매개변수와 같이 암호시스템의 안전성을 달성하기 위해 필수적으로 사용된다. 암호학적으로 안전한 난수발생기의 안전성은 난수성의 원천이라 할 수 있는 잡음원의 엔트로피에 근본적으로 의존하며, 대표적인 엔트로피 추정법으로는 미국 NIST의 SP 800-90B가 널리 알려져 있다. 그런데 NIST의 엔트로피 추정법은 기본적으로 잡음원의 분포가 변하지 않음을 가정하고 설계된 까닭에 SP 800-90B 문서 상에는 잡음원의 분포 변화를 확인하는 방법이 명시되어 있지 않다. 본 논문에서는 잡음원의 분포 변화를 탐지할 수 있는 방법을 제시한다. 제안하는 방법은 잡음원의 통계적 특성이 IID인 경우와 마르코프 특성을 가지는 Non-IID인 경우를 포함하고 있다. 또한, 여러 시뮬레이션을 통해 제안한 분포 변화 탐지법의 유효성을 실험적으로 확인한다.

키워드 : 분포 변화, 정류성, 잡음원, 엔트로피 소스, 난수발생기
Key Words : Changing distribution, Stationary, Noise source, Entropy source, Random number generator

ABSTRACT

For a secure cryptosystem, it is necessary to use cryptographically secure random numbers, which are used as crypto keys and parameters of security protocols. The security of cryptographically secure random number generators intrinsically relies on the entropy of the noise source, the root of randomness. NIST SP 800-90B is a representative entropy estimation method for noise sources. However, the NIST method does not specify how to test the stationarity of noise sources, since it is designed under the assumption of the stationarity of the distribution of the noise sources. In this paper, we propose methods to detect changing distribution for noise sources in the cryptographically secure random number generators. The proposed methods are designed to detect changing distribution for the IID noise sources and the Non-IID noise sources with Markov chain property. Furthermore, we provide various simulations to examine the proposed methods.

◆ First Author : Kookmin University Department of Financial Information Security, ruokay@kookmin.ac.kr, 정회원
° Corresponding Author : Kookmin University Department of Information Security, Cryptology, and Mathematics, jskang@kookmin.ac.kr, 종신회원
* Kookmin University Department of Financial Information Security, tnwls1595@kookmin.ac.kr, 학생회원,
** Kookmin University Department of Information Security, Cryptology, and Mathematics, salt@kookmin.ac.kr, 종신회원
논문번호 : 202103-047-A-RE, Received February 25, 2021; Revised April 19, 2021; Accepted April 21, 2021

Ⅰ. 서 론

암호통신 시스템에서 난수는 암호키(secret key), 논스(nonce), 암호학적 솔트(cryptographic salt), 프로토콜의 파라미터(parameter) 등 암호 목적으로 사용된다. 암호통신 시스템의 안전성은 안전한 난수 사용에 의존하며, 이와 같이 암호 목적으로 사용되는 난수는 반드시 암호학적 난수발생기(cryptographically secure random number generator)에서 생성되어야 안전성을 보장받을 수 있다[1]. 암호학적 난수발생기는 그림 1과 같이 진난수발생기(True random number generator, TRNG)와 의사난수발생기(Pseudo random number generator, PRNG) 두 단계로 구성된다[2, 3]. 진난수발생기는 예측 불가능성의 근원인 잡음원(noise source)으로부터 씨드(seed)를 생성하며[4], 의사난수발생기는 씨드를 결정론적 알고리즘에 입력하여 암호학적 난수를 생성한다[5].

난수의 안전성 평가 방법은 통계적 난수성 평가(statistical randomness test)와 엔트로피 추정(entropy estimation)으로 나뉜다. 통계적 난수성 평가는 암호학적 난수발생기의 최종 출력수열이 랜덤수열과 구별되는지 판정하는 방법이며, 미국 NIST의 SP 800-22[6]와 독일 BSI의 AIS.20[7]과 AIS.31[8]이 대표적인 통계적 난수성 평가 방법이다. 엔트로피 추정은 암호학적 난수발생기의 입력인 잡음원의 예측 불가능성을 정량적으로 추정하는 방법으로, 미국 NIST의 SP 800-90B[4]가 대표적인 방법이다. 한편, 통계적 난수성 평가 방법은 암호학적 안전성을 보장할 수 없으며[6], 암호학적 난수발생기의 본질적인 안전성은 잡음원의 예측 불가능성에 전적으로 의존하기 때문에[4], 최근에는 엔트로피 추정법을 중심으로 연구가 활발히 진행되고 있다.

NIST의 엔트로피 추정법인 SP 800-90B는 잡음원의 엔트로피를 보수적으로 추정하고, 최적 예측 공격(optimum guessing attack)량과의 관계를 근거로 최소 엔트로피(min-entropy)를 예측 불가능성의 측도로 사용한다. 또한, NIST SP 800-90B는 잡음원의 분포가 변하지 않는다는 정류성(stationarity)을 가정하여 엔트로피 추정법을 설계하였음을 명시하고 있다[4]. 하지만, 잡음원의 분포가 변하는 환경에서는 NIST의 엔트로피 추정법을 직접 적용하는 것은 합리적이지 않다. 또한, 이러한 단점을 보완하기 위해 최근에는 중국과학원(Chinese academy of sciences)에서 신경망을 이용하여 시간에 따라 분포가 변하는 시간 의존적(time-varing) 잡음원의 엔트로피를 추정하기 위한 연구를 진행하였다[9, 10]. 중국과학원의 연구[10]에서는 데이터 열(data stream)의 분포 변화 시점을 찾는 알고리즘인 ADWIN2[11]를 활용하여 분포 변화 시점을 찾고, 엔트로피를 추정하는 방식을 취하고 있다. 하지만, ADWIN2의 논문을 참고했을 때, 이 방법은 연속형 자료(continuous data)의 분포 변화 시점을 검출하는 것으로 보이며, 이는 이산형 자료(discrete data)인 잡음원 출력수열에 직접 적용하는 것은 적합하지 않은 것으로 보인다.

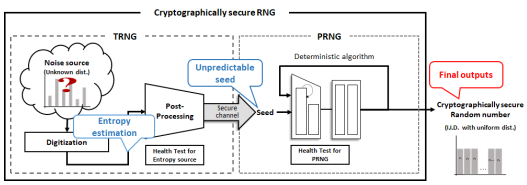

그림 1. 암호학적 난수발생기의 구조
Fig. 1. The structure of a cryptographically secure random number generator

1.1 논문의 기여

본 논문에서는 다른 시간에 생성된 잡음원의 두 출력수열로부터 잡음원의 분포 변화가 발생했는지 탐지할 수 있는 방법을 제안한다. 제안하는 방법은 잡음원의 통계적 특성이 I.I.D.(Independent and identically distributed, 이하 IID)인지 아닌지에 따라 다른 방법이 적용된다. 논문의 주요결과를 정리하면 아래와 같다.

- 헬스 테스트와 재시작 검정이 분포 변화 탐지법으로 활용되기 어려운 이유를 제시한다.
- IID 통계적 특성을 가지는 잡음원의 분포 변화 탐지법을 제안한다.
- Non-IID 통계적 특성 중에서 대표적으로 마르코프 성질을 따르는 분포 관점의 잡음원 분포 변화 탐지법을 제안한다.

한편, 기존의 엔트로피 추정법은 잡음원의 정류성을 가정하고 있지만, 정류성을 확인하는 방법과 절차를 제시하지 않고 있다. 이에 제안하는 방법은 기존 엔트로피 추정법을 보완할 수 있는 잡음원 분포 변화 탐지법으로 활용될 수 있다고 기대한다.

1.2 논문의 구성

논문은 총 6 장으로 구성되며, 논문의 나머지는 다음과 같이 구성된다. 2 장에서는 NIST 엔트로피 추정법을 간단히 소개하고, 기존 엔트로피 저하 탐지방법

이 분포 변화 탐지법으로 활용되기에는 부족하다는 점을 밝힌다. 3 장에서는 IID로 판정된 잡음원의 분포 변화 탐지법의 설계 원리와 세부적인 탐지 방법을 제안한다. 4 장에서는 Non-IID 중 마르코프 특성을 갖는 잡음원의 분포 변화 탐지법의 설계 원리와 세부적 탐지 기법을 제시한다. 5 장에서는 제안하는 방법을 실험적으로 분석한 결과를 제시하며, 마지막으로 6 장에서 논문의 결론을 맺는다.

Ⅱ. NIST 엔트로피 추정법과 분포 변화 탐지

NIST의 SP 800-90B는 암호모듈검증제도(Cryptography Module Validation Program, CMVP)에서 암호학적 난수발생기 내 잡음원의 엔트로피 검증 방법으로 활용된다. NIST의 엔트로피 추정법은 잡음원의 분포가 변하지 않는 정류성을 가정하고 설계되었다. 또한, 잡음원의 엔트로피 저하를 탐지하는 방법을 활용하여 난수발생기가 잡음원에서 엔트로피를 안정적으로 수집하는지 확인하고 있다. 본 장에서는 NIST SP 800-90B를 소개하고, 헬스 테스트와 재시작 검정을 분포 변화 관점에서 분석한다. 2 장의 1 절에서는 NIST SP 800-90B의 개요를 소개하고, 잡음원의 엔트로피 저하를 탐지하는 헬스 테스트와 재시작 검정을 소개한다. 2 절에서는 위 두 방법이 잡음원의 엔트로피 저하가 발생하지 않는 분포 변화를 탐지할 수 없음을 실험으로 검증하고, 3 절에서 기존 방법을 보완할 수 있는 새로운 분포 변화 탐지법의 필요성과 설계를 제시한다.

2.1 NIST SP 800-90B 개요

NIST SP 800-90B는 암호학적 난수발생기의 엔트로피 소스 설계와 잡음원 검증을 위한 엔트로피 추정법을 다루고 있다. NIST는 암호학적 난수발생기의 엔트로피 소스 모델을 그림 2와 같이 제시하고 있으며, 잡음원, 컨디셔닝(conditioning component), 헬스 테스트(health test)로 구성된다.

잡음원은 난수발생기의 예측불가능성의 근원이며, 컨디셔닝은 잡음원의 편향성을 줄이고 엔트로피 비율(entropy rate)을 올리는 역할을 하고, 헬스 테스트는 추정된 잡음원의 엔트로피가 유지되는지 판정하는 방법이다. 이때, NIST는 잡음원의 분포가 변하지 않는다는 가정에서 엔트로피 추정법을 설계하였다[4]. NIST의 엔트로피 추정은 분포 판정(determine the track), 엔트로피 추정(estimate entropy), 엔트로피 갱신(update entropy estimate)의 세 단계로 진행된다.

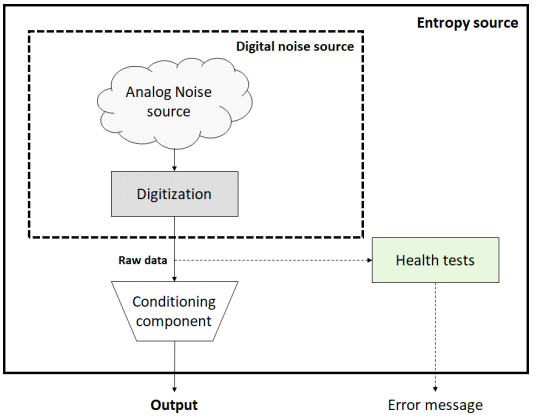

그림 2. NIST의 엔트로피 소스 모델
Fig. 2. The NIST's entropy source model

분포 판정은 잡음원의 분포가 IID인지 Non-IID인지 확인하는 단계이다. 엔트로피 추정은 IID 판정여부에 따라 IID track과 Non-IID track으로 나뉘어 잡음원의 샘플 당 엔트로피를 추정하는 단계이다. 엔트로피 갱신은 난수발생기를 1,000번 재시작하여 획득한 잡음원을 이용한 재시작 검정(restart test)과 컨디셔닝 적용 유·무에 따라 엔트로피를 갱신하는 단계이다. 이 중 NIST의 헬스 테스트와 재시작 검정이 분포 변화 탐지법으로 활용 가능한지 확인하기 위한 분석을 진행한다.

2.1.1 헬스 테스트

NIST의 헬스 테스트는 잡음원의 추정된 엔트로피에 기반하여, 잡음원이 기대와 같이 동작하는지 확인하기 위해 진행하는 실시간 검사이다[4]. 예를 들어, 추정된 잡음원의 샘플 당 최소엔트로피가 0.5라면, 특정 샘플 값이 발생할 최대 확률은 $2^{-0.5}$이다. NIST는 최대 발생 확률에 기반하여 특정 값이 비이상적으로 연속 발생하는지 확인하는 연속 발생 횟수 검정(repetition count test)과 환경 변화로 인해 특정 시간 내에서 특정 값이 많이 발생하여 엔트로피가 저하되는 현상을 확인하는 구간 내 발생비율 검정(adaptive proportion test)을 헬스 테스트로 권고한다.

2.1.2 재시작 검정

재시작 검정은 난수발생기를 1,000 회 재시작하여 수집한 1,000,000 개의 표본으로 진행되며, 수집한 표본은 그림 3과 같이 행렬 M으로 구성한다. 재시작 검정의 목적은 재시작한 난수발생기에서 수집한 잡음원 사이에 연관성이 존재하는 취약점을 검출하기 위함이

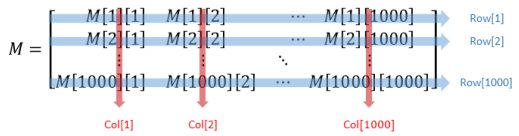

그림 3. 재시작 검정 데이터의 구조
Fig. 3. The data structure of restart test

다. 재시작 검정은 건전성 검사(sanity check) 단계와 엔트로피 갱신 단계로 구성되며, 두 단계가 모두 통과되어야 잡음원의 엔트로피 검증이 진행된다.

건전성 검사는 재시작 검정 전에 추정된 잡음원의 엔트로피 H_I보다 재시작을 통해 수집된 잡음원 표본 값의 발생빈도가 많이 발생하는지 확인하는 단계이다. 이때, 특정 값의 발생빈도가 높은 경우는 가정된 잡음원의 분포 유지에 실패했다고 판정한다. 엔트로피 갱신 단계는 행 데이터(row data)의 최소엔트로피 H_r과 열 데이터(column data)의 최소엔트로피 H_c의 중 작은 값이 H_I의 절반 이하로 떨어지는지 확인하는 단계이다. 즉, $\min\{H_r, H_c\} < \frac{1}{2}H_I$이면, 난수발생기의 재시작으로 인해 종속성이 발생했다고 판정하고 탈락시키고, 그렇지 않은 경우, 잡음원의 엔트로피를 $H = \min\{H_r, H_c, H_I\}$로 갱신하고 검증을 진행한다.

2.2 분포 변화 관점의 헬스 테스트와 재시작 검정 분석

본 절에서는 헬스 테스트와 재시작 검정이 잡음원의 분포 변화 탐지법으로 활용될 수 있는지 확인하기 위한 실험적 분석을 진행한다. 본 절의 분석은 NIST 재시작 검정의 분포 변화 탐지 관점의 연구결과[12]를 활용하여 진행하였다. 헬스 테스트와 재시작 검정이 엔트로피 저하가 발생하는 분포 변화를 검출하기 위해 설계되었기 때문에, 엔트로피 저하가 발생하지 않는 분포 변화를 검출하기 어려울 것으로 분석했다. 이를 검증하기 위해 엔트로피가 저하가 발생한 분포 변화를 시나리오 1, 엔트로피 저하가 발생하지 않은 분포 변화를 시나리오 2로 나누어 실험을 구성하였으며, 다음과 같은 가정에서 실험적 분석을 진행하였다. 잡음원 표본은 2 비트 크기로 출력되며, NIST의 분포 판정법을 통해 IID로 판정되었다고 가정하자. 잡음원의 표본공간 S는 $S = \{00, 01, 10, 11\}$이며, $s \in S$에 대해 난수발생기가 정상 동작하는 경우에는 식 (1)과 같은 분포를 따른다고 하자.

$$P(X=s) = \begin{cases} 0.6 & , \text{if } s = 00, \\ 0.13 & , otherwise. \end{cases} \quad (1)$$

암호시스템에서 난수발생기를 사용하는 중 온도, 전압 등 물리적 변화가 발생하거나[13], 시스템의 안전성을 위협하기 위한 진난수발생기에 대한 공격[14-16], 장비의 노후화[17] 등에 의해 구동 환경이 변화하여 잡음원 출력분포가 영향을 받을 수 있다. 이때, 잡음원의 엔트로피 저하가 발생한 분포 변화와 엔트로피 저하가 발생하지 않은 분포 변화가 발생한 경우로 나누어 검증을 진행하였다. 난수발생기 구동 환경 변화로 인해 정상 동작과 달리, 표본 값 00이 발생할 확률이 $P(X=00)=0.7$로 높아진 경우, 엔트로피 저하가 발생한 분포 변화이며, 표본 값 00이 발생할 확률과 01이 발생할 확률이 $P(X=00)=0.1\dot{3}$과 $P(X=01)=0.6$로 바뀌는 경우를 엔트로피 저하가 발생하지 않은 분포 변화이다. 두 시나리오에 대해 헬스 테스트와 재시작 검정을 적용한 결과는 표 1과 같다. 두 방법은 엔트로피 저하를 검출하기 위해 설계된 방법이기 때문에, 2.2 절의 실험 결과는 엔트로피 저하가 발생하지 않은 경우의 분포 변화를 탐지하기 어려울 것이라는 분석을 실험적으로 검증한 결과이다.

표 1. 시나리오에 따른 헬스 테스트와 재시작 검정의 분포 변화 탐지 결과
Table 1. Detecting distribution change of the health test and the restart test by the scenarios

Test / Scenario	Health test	Restart test
Scenario 1	Detection	Detection
Scenario 2	Non-detection	Non-detection

2.3 새로운 잡음원 분포 판정법 설계

NIST 엔트로피 추정은 잡음원의 분포가 변하지 않는다는 가정에서 설계되었으며, IID를 확인하는 분포 판정법과 이에 따라 엔트로피를 계산하는 절차로 진행된다. 하지만, 암호통신 시스템에서 난수발생기를 사용하는 중 잡음원 수집 환경에 변화가 발생할 수 있으며, 2.2 절을 통해 기존 방법으로는 엔트로피가 저하되지 않는 분포 변화를 탐지하기 어려움을 확인했다. 이에 기존 방법을 보완할 수 있는 분포 변화 탐지 방법을 설계한다. 설계한 방법은 그림 4와 같이 설계된 잡음원(Data 1)의 통계적 특성이 IID인지 아닌지에 따라 다른 방법이 적용된다. 이때, 잡음원의 정류성을 검사하기 위해서 난수발생기 구동환경의 변화나 공격 징후가 포착되는 등과 같이 시간 t가 지난 후 잡

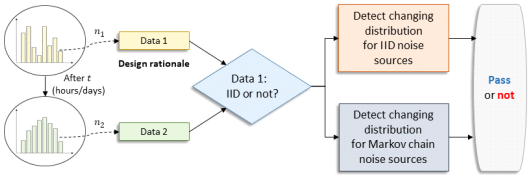

그림 4. 잡음원의 정류성 검사 설계
Fig. 4. The design of stationarity test for noise source

음원을 수집하고, 수집한 데이터(Data 2)로 잡음원의 분포 변화를 확인한다. IID인 경우의 분포 변화 탐지법은 3 장, 마르코프 체인인 경우의 분포 변화 탐지법은 4 장에서 구체적으로 제시한다.

Ⅲ. IID 잡음원 분포 변화 탐지법 설계

엔트로피 저하를 탐지하는 기존의 방법으로는 잡음원의 정류성이 깨짐을 온전히 판정할 수 없음을 2 장에서 검증하였다. 3 장에서는 IID로 판정된 잡음원을 대상으로 하는 분포 변화 탐지법을 제안한다. 3.1 절에서는 제안하는 방법의 설계 원리를 소개하고, 3.2 절에서는 설계한 IID 잡음원의 분포 변화 탐지법을 설명한다.

3.1 IID 잡음원의 분포 변화 탐지법 설계 원리

IID로 판정된 잡음원의 분포 변화 탐지법은 두 분포가 같은지 판정하는 여러 모집단의 동질성 검정(homogeneous test)과 설정한 유의수준 α 하에서 분포 변화를 통계적으로 판정하는 가설검정법(hypothesis test)을 원리로 두고 있다. 제안한 IID 잡음원의 분포 변화 탐지법은 설계된 잡음원 출력의 분포와 특정 시간 후에 출력된 잡음원 출력의 분포가 달라졌는지 확인하는 방법이다. 이때, 두 분포가 변했는지 통계적으로 판정하는 데 가설검정법이 사용되며, 설정된 귀무가설 H_0 는 "두 분포는 같다"이며, 이에 상정되는 대립가설 H_1 은 "H_0 가 아니다"로 설정된다.

제안하는 방법은 잡음원 분포 변화 탐지의 효율성을 위해 그림 5와 같이 두 개의 단계로 설계하였다. 1 단계 카이제곱 검정은 전반적인 분포 변화를 탐지하여 변화가 큰 경우를 걸러내는 역할을 하고, 2 단계 두 모비율 검정은 두 모집단에서 발생 가능한 모든 표본값의 발생비율을 비교하기 때문에 1 단계보다 엄밀하게 분포 변화를 탐지한다. 예를 들어 표본의 크기가 8 비트인 경우, 1 단계 검정에서는 하나의 카이제곱 통계량을 계산하여 전반적인 분포 변화를 탐지하지만, 2 단계 검정에서는 256 개의 표본공간을 모두 조사하여

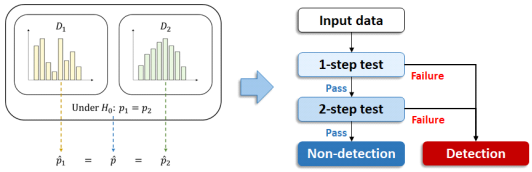

그림 5. 제안하는 IID 잡음원의 분포 변화 탐지법 설계
Fig. 5. The proposed method for IID noise sources to detect changing distribution

분포 변화를 탐지한다. 이때, IID 잡음원의 분포 변화 탐지법은 1 단계와 2 단계를 모두 통과한 경우에 한해서만 잡음원의 분포 변화가 없다고 판정한다.

3.2 IID 잡음원의 분포 변화 탐지법 설계

IID로 판정된 잡음원의 분포 변화 탐지법은 두 분포가 같은지 판정하는 여러 모집단의 동질성 검정(homogeneous test)과 설정한 유의수준 α 하에서 분포 변화를 통계적으로 판정하는 가설검정법(hypothesis test)을 원리로 두고 있다. 제안한 IID 잡음원의 분포 변화 탐지법은 설계된 잡음원 출력의 분포와 특정 시간 후에 출력된 잡음원 출력의 분포가 달라졌는지 확인하는 방법이다. 이때, 두 분포가 변했는지 통계적으로 판정하는 데 가설검정법이 사용되며, 설정된 귀무가설 H_0 는 "두 분포는 같다"이며, 이에 상정되는 대립가설 H_1 은 "H_0 가 아니다"로 설정된다.

1 단계 카이제곱 검정은 범주형 자료의 두 모집단의 비교를 기반으로 설계하였으며, 2 단계는 두 모비율 검정을 기반으로 설계하였다. 분포에 무관한(distribution free) 두 모집단을 D_1 과 D_2 라고 하자. D_1 과 D_2 에서 랜덤하게 추출한 n_1 개, n_2 개의 표본의 확률변수를 각각 $X_1^{(1)}, X_2^{(1)}, \ldots, X_{n_1}^{(1)}$, $X_1^{(2)}, X_2^{(2)}, \ldots, X_{n_2}^{(2)}$ 로 표현하자. D_1 과 D_2 의 표본공간을 S라 할 때, 각 모집단에서 고정된 표본 값 $k \in S$가 발생할 확률을 $p_k^{(1)}$ 과 $p_k^{(2)}$ 라 하자. IID 잡음원의 분포 변화 탐지법에서 설정한 귀무가설 H_0 와 대립가설 H_1 은 아래와 같다.

H_0 : 모든 $k \in S$에 대하여 $p_k^{(1)} = p_k^{(2)}$ 가 성립한다.
H_1 : H_0 가 아니다.

$i \in \{1,2\}$ 인 i 와 $1 \le j \le |S|$ 인 j 에 대하여, 1 단계 카이제곱 검정은 추정 기대도수(estimated expected frequency) $\hat{E}_j^{(i)}$ 와 관측도수 $O_j^{(i)}$ 의 차이를

이용하여 분포 변화를 탐지하는 방법으로 카이제곱 통계량을 활용하며, 추출한 표본의 수인 n_1과 n_2가 충분히 크면 식 (2)에 제시한 것과 같이 자유도가 $(2-1)(|S|-1)$인 카이제곱 분포에 근사한다. 즉,

$$\chi^2 = \sum_{i=1}^{2}\sum_{j=1}^{|S|}\frac{\left(O_j^{(i)}-\hat{E}_j^{(i)}\right)^2}{\hat{E}_j^{(i)}} \sim \chi^2(|S|-1). \qquad (2)$$

이때, 1 단계의 분포 변화 탐지는 다음과 같이 진행된다. 카이제곱 검정통계량을 χ_0^2, 설정된 유의수준을 $\alpha^{(1)}$라 하면, 유의확률 P가 유의수준 $\alpha^{(1)}$보다 작은 경우인 $P=P(\chi^2 \geq \chi_0^2) < \alpha^{(1)}$ 또는 χ_0^2가 유의수준 $\alpha^{(1)}$의 기각역보다 큰 경우인 $\chi_0^2 \geq \chi_{\alpha^{(1)}}^2(|S|-1)$에 통계적으로 분포가 변화했다고 판정한다.

2 단계 두 모비율 검정은 고정된 $k \in S$에 대해 $H_0 : p_k^{(1)} = p_k^{(2)}$가 참일 때, 검정통계량 Z가 표준정규분포에 근사하는 성질을 이용하는 방법이다. X를 n_1개의 표본에서 k가 발생한 수, Y를 n_2개의 표본에서 k가 발생한 수를 의미하는 확률변수라 하면, X는 크기가 n_1이고 확률이 $p_k^{(1)}$인 이항분포 $X \sim B\left(n_1, p_k^{(1)}\right)$를 따르고, Y는 크기가 n_2이고 확률이 $p_k^{(2)}$인 이항분포 $Y \sim B\left(n_2, p_k^{(2)}\right)$를 따른다. $p_k^{(1)}, p_k^{(2)}$의 추정치를 $\hat{p}_1 = \frac{X}{n_1}$, $\hat{p}_2 = \frac{Y}{n_2}$라 하면, 귀무가설 H_0하에서 p의 추정치는 합동표본비율(pooled sample proportion)인 $\hat{p} = \frac{X+Y}{n_1+n_2}$가 되고, 분산 추정치 $Var\left(\hat{p}_1-\hat{p}_2\right)$는 $Var\left(\hat{p}_1-\hat{p}_2\right) = \hat{p}\left(1-\hat{p}\right)\left(n_1^{-1}+n_2^{-1}\right)$로 쓸 수 있다[18]. 이때, n_1과 n_2가 충분히 크면 식 (3)에 제시한 것과 같이 통계량은 표준정규분포 $N(0,1)$에 근사한다.

$$Z = \frac{\left(\hat{p}_1-\hat{p}_2\right)}{\sqrt{\hat{p}\left(1-\hat{p}\right)\left(n_1^{-1}+n_2^{-1}\right)}} \sim N(0,1). \qquad (3)$$

2 단계의 분포 변화 탐지는 다음과 같이 진행된다. 계산된 통계량을 z, 설정된 유의수준을 $\alpha^{(2)}$라 하면, 유의확률 P가 설정된 유의수준 $\alpha^{(2)}$보다 작은 경우인 $P=P(|Z| \geq |z|) < \alpha^{(2)}$ 또는 z가 유의수준 $\alpha^{(2)}$의 기각역보다 큰 경우인 $|z| \geq z_{\alpha^{(2)}/2}$일 때, 잡음원의 분포 변화가 발생했다고 판정한다.

Ⅳ. 마르코프 잡음원의 분포 변화 탐지법 설계

잡음원의 통계적 특성이 IID인지 또는 Non-IID인지 판별 후 엔트로피 추정이 진행된다. 3 장에서 제안한 방법은 IID로 판정된 잡음원에 대해서만 분포 변화를 탐지하는 방법으로, Non-IID로 판정된 잡음원에 적용할 수 있는 분포 변화 탐지법이 필요하다. 하지만, Non-IID 특성은 하나의 특성으로 한정하기 어렵기 때문에, 4 장에서는 대표적인 Non-IID 특성인 마르코프 특성을 가지는 잡음원의 분포 변화 탐지법을 제안한다. 4.1 절에서는 제안하는 마르코프 특성의 분포 변화 탐지법의 설계 원리인 마르코프 체인의 정류성 검사를 소개하고, 4.2 절에서는 설계한 마르코프 특성 잡음원의 분포 변화 탐지법을 설명한다.

4.1 마르코프 체인의 정류성 검사

Non-IID로 판정된 잡음원은 IID로 판정된 잡음원과 달리 특정한 성질로 규정할 수 없기 때문에, 4.1 절에서는 대표적인 Non-IID 특성인 1 차 마르코프 체인(1st order Markov chain)을 대상으로 한 분포 변화 탐지법을 제안한다. 제안하는 방법은 두 분포에서 전이횟수(transition count)의 발생비율을 비교하는 방법과 두 분포의 전이확률 추정을 이용한 방법으로, Billingsley의 1 차 마르코프 체인의 정류성 검사(stationary test on the 1st order Markov chain)[19]를 Non-IID로 판정된 잡음원의 분포 탐지 방법에 활용한 것이다. 1 차 마르코프 체인의 정류성 검사는 다음의 원리로 설계되었다. 초기확률(initial probability)이 p_j이고, 전이확률(transition probability)이 p_{jk}인 1 차 마르코프 체인에서 생성된 표본수열을 $\{x_1, x_2, ..., x_n\}$라 하자. s를 표본공간의 크기, j, k를 $j,k \in [0, s-1]$인 정수라 할 때, 크기가 $s \times s$인 행렬 $F = \{f_{jk}\}$는 표본수열에서 j가 발생한 다음 k가 발생한 전이횟수를 의미한다고 하자. 1 차 마르코프 체인의 정류성 검사는 식 (4)에 제시한 것과 같이 카이제곱 통계량을 이용하며, 통계량이 자유도가 $s(s-1)$인 카이제곱 분포에 근사함을 이용한다. 즉,

$$\chi^2 = \sum_{j=0}^{s-1}\sum_{k=0}^{s-1}\frac{\left(f_{jk}-f_{j\cdot}p_{jk}\right)^2}{f_{j\cdot}p_{jk}} \sim \chi^2(s(s-1)). \qquad (4)$$

여기서 $f_{j\cdot}$는 $f_{j\cdot} = f_{j0}+f_{j1}+\cdots+f_{j(s-1)}$을 의미한다.

4.2 마르코프 특성 잡음원의 분포 변화 탐지법 설계

잡음원 표본의 크기는 1 비트이고 잡음원의 출력분포가 1 차 마르코프 체인을 따른다고 가정하자. $m \geq 0$ 인 m 에 대하여, X_m 을 m 번째 상태(state)를 나타내는 확률변수라 하면, 표본공간의 크기가 2인 1 차 마르코프 체인 특성을 가지는 D_1 과 D_2 의 전이확률은 식 (5)에 제시한 것과 같이 각각 전이행렬(transition matrix) T_1 과 T_2 로 표현한다. 즉,

$$T_1 = \begin{pmatrix} p_{00}^{(1)} & p_{01}^{(1)} \\ p_{10}^{(1)} & p_{11}^{(1)} \end{pmatrix}, \quad T_2 = \begin{pmatrix} p_{00}^{(2)} & p_{01}^{(2)} \\ p_{10}^{(2)} & p_{11}^{(2)} \end{pmatrix}. \tag{5}$$

여기서, m 번째 상태를 $j \in \{0,1\}$, $(m+1)$ 번째 상태를 $k \in \{0,1\}$ 라 하면, $i \in \{1,2\}$ 에 대하여 D_i 의 전이행렬 T_i 는 전이확률 $P_i(X_{m+1} = k \mid X_m = j) = p_{jk}^{(i)}$ 로 표현되며, $p_{00}^{(i)} + p_{01}^{(i)} = 1$, $p_{10}^{(i)} + p_{11}^{(i)} = 1$ 을 만족한다.

1 차 마르코프 체인 특성을 가지는 잡음원의 분포 변화를 탐지하기 위한 귀무가설 H_0 와 대립가설 H_1 은 아래와 같이 설정한다.

H_0 : 모든 j,k 에 대하여 $p_{jk}^{(1)} = p_{jk}^{(2)}$ 가 성립한다.
H_1 : H_0 가 아니다.

즉, 귀무가설은 두 분포의 전이행렬이 같음을 의미하는 $H_0 : T_1 = T_2$ 로 표현할 수 있으며, 대립가설은 두 분포의 전이행렬이 같지 않음을 의미하는 $H_1 : T_1 \neq T_2$ 로 표현할 수 있다. 이때, 모든 $j,k \in \{0,1\}$ 에 대해서 전이확률이 같다고 판정된 경우인 귀무가설 $H_0 : T_1 = T_2$ 가 채택되면 통계적으로 분포가 같다고 판정한다. 1 차 마르코프 특성 잡음원의 분포 변화 탐지에서 관측값을 χ_0^2, 설정된 유의수준을 α 라 하면, 가설검정법을 활용하여 유의확률 P 가 유의수준 α 보다 작은 경우인 $P = P(\chi^2 \geq \chi_0^2) < \alpha$ 또는 χ_0^2 가 유의수준 α 의 기각역보다 큰 경우인 $\chi_0^2 \geq \chi_\alpha^2(|S|-1)$ 에 통계적으로 분포가 변화했다고 판정한다.

4.2.1 분할표를 이용한 분포 변화 탐지 기법

마르코프 체인 특성을 가지는 잡음원의 분포 변화 탐지는 4 개의 범주로 나누어진 2 개의 모집단을 관측한 결과로 표 2와 같은 2×4 분할표로 표현할 수 있다.

표 2. 마르코프 특성의 잡음원의 분포 변화 탐지법에 사용되는 2×4 분할표
Table 2. The 2×4 contingency table of the method for the noise sources with Markov chain properties

D_i \ (j,k)	(0,0)	(0,1)	(1,0)	(1,1)	Sum
D_1	$f_{00}^{(1)}$	$f_{01}^{(1)}$	$f_{10}^{(1)}$	$f_{11}^{(1)}$	$n_1 - 1$
D_2	$f_{00}^{(2)}$	$f_{01}^{(2)}$	$f_{10}^{(2)}$	$f_{11}^{(2)}$	$n_2 - 1$
Sum	e_{00}	e_{01}	e_{10}	e_{11}	$n_1 + n_2 - 2$

$j,k \in \{0,1\}$ 인 j,k 에 대해, 귀무가설 H_0 가 참이라는 가정하에서, 전체 표본수열에서 각 범주의 발생비율 $p_{jk}^{(1)} = p_{jk}^{(2)} = p_{jk}$ 의 추정값 $\hat{p}_{jk}$ 은 식 (6)과 같이 쓸 수 있다.

$$\hat{p}_{jk} = \frac{f_{jk}^{(1)} + f_{jk}^{(2)}}{n_1 - 1 + n_2 - 1} = \frac{e_{jk}}{n_1 + n_2 - 2}. \tag{6}$$

이를 이용하여 분포 D_i 에서 m 번째 상태 j 와 $(m+1)$ 번째 상태 k 가 발생할 추정 기대도수 $\hat{E}_{jk}^{(i)}$ 를 계산하면 식 (7)과 같다.

$$\begin{aligned} \hat{E}_{jk}^{(1)} &= (n_1 - 1)\hat{p}_{jk} = \frac{(n_1 - 1)e_{jk}}{n_1 + n_2 - 2}, \\ \hat{E}_{jk}^{(2)} &= (n_2 - 1)\hat{p}_{jk} = \frac{(n_2 - 1)e_{jk}}{n_1 + n_2 - 2}. \end{aligned} \tag{7}$$

두 모집단의 동질성 검정은 관측도수 $f_{jk}^{(i)}$ 와 추정 기대도수 $\hat{E}_{jk}^{(i)}$ 의 차이를 이용하는 카이제곱 검정법이 사용되며, n_1 과 n_2 가 충분히 크면 식 (8)에 제시한 것과 같이 자유도가 $((2-1)(4-1))$ 인 카이제곱 분포에 근사한다. 즉,

$$\sum_{i=1}^{2}\sum_{j=0}^{1}\sum_{k=0}^{1} \frac{\left(f_{jk}^{(i)} - \hat{E}_{jk}^{(i)}\right)^2}{\hat{E}_{jk}^{(i)}} \sim \chi^2(3). \tag{8}$$

4.2.2 전이행렬을 이용한 분포 변화 탐지 기법

전이행렬 추정을 활용하여 마르코프 체인에서 추출된 두 분포의 변화를 탐지할 수 있다. 이때, 각 분포의 전이확률은 식 (9)와 같이 추정한다.

$$\hat{p}_{00}^{(1)} = \frac{f_{00}^{(1)}}{f_{00}^{(1)}+f_{01}^{(1)}}, \quad \hat{p}_{00}^{(2)} = \frac{f_{00}^{(2)}}{f_{00}^{(2)}+f_{01}^{(2)}},$$
$$\hat{p}_{01}^{(1)} = \frac{f_{01}^{(1)}}{f_{00}^{(1)}+f_{01}^{(1)}}, \quad \hat{p}_{01}^{(2)} = \frac{f_{01}^{(2)}}{f_{00}^{(2)}+f_{01}^{(2)}},$$
$$\hat{p}_{10}^{(1)} = \frac{f_{10}^{(1)}}{f_{10}^{(1)}+f_{11}^{(1)}}, \quad \hat{p}_{10}^{(2)} = \frac{f_{10}^{(2)}}{f_{10}^{(2)}+f_{11}^{(2)}},$$
$$\hat{p}_{11}^{(1)} = \frac{f_{11}^{(1)}}{f_{10}^{(1)}+f_{11}^{(1)}}, \quad \hat{p}_{11}^{(2)} = \frac{f_{11}^{(2)}}{f_{10}^{(2)}+f_{11}^{(2)}}. \tag{9}$$

H_0가 참이라는 가정하에서 $\hat{p}_{jk} = \hat{p}_{jk}^{(1)} = \hat{p}_{jk}^{(2)}$ 이며, 각 확률의 추정치는 식 (10)과 같이 쓸 수 있다.

$$\hat{p}_{00} = \frac{f_{00}^{(1)}+f_{00}^{(2)}}{f_{00}^{(1)}+f_{01}^{(1)}+f_{00}^{(2)}+f_{01}^{(2)}},$$
$$\hat{p}_{01} = \frac{f_{01}^{(1)}+f_{01}^{(2)}}{f_{00}^{(1)}+f_{01}^{(1)}+f_{00}^{(2)}+f_{01}^{(2)}},$$
$$\hat{p}_{10} = \frac{f_{10}^{(1)}+f_{10}^{(2)}}{f_{10}^{(1)}+f_{11}^{(1)}+f_{10}^{(2)}+f_{11}^{(2)}},$$
$$\hat{p}_{11} = \frac{f_{11}^{(1)}+f_{11}^{(2)}}{f_{10}^{(1)}+f_{11}^{(1)}+f_{10}^{(2)}+f_{11}^{(2)}}. \tag{10}$$

두 모집단 D_1과 D_2에서 발생할 추정 기대도수 $\hat{E}_{jk}^{(1)}$과 $\hat{E}_{jk}^{(2)}$를 계산하면 식 (11)과 같다.

$$\hat{E}_{00}^{(1)} = \left(f_{00}^{(1)}+f_{01}^{(1)}\right)\hat{p}_{00}, \quad \hat{E}_{01}^{(1)} = \left(f_{00}^{(1)}+f_{01}^{(1)}\right)\hat{p}_{01},$$
$$\hat{E}_{10}^{(1)} = \left(f_{10}^{(1)}+f_{11}^{(1)}\right)\hat{p}_{10}, \quad \hat{E}_{11}^{(1)} = \left(f_{10}^{(1)}+f_{11}^{(1)}\right)\hat{p}_{11},$$
$$\hat{E}_{00}^{(2)} = \left(f_{00}^{(2)}+f_{01}^{(2)}\right)\hat{p}_{00}, \quad \hat{E}_{01}^{(2)} = \left(f_{00}^{(2)}+f_{01}^{(2)}\right)\hat{p}_{01},$$
$$\hat{E}_{10}^{(2)} = \left(f_{10}^{(2)}+f_{11}^{(2)}\right)\hat{p}_{10}, \quad \hat{E}_{11}^{(2)} = \left(f_{10}^{(2)}+f_{11}^{(2)}\right)\hat{p}_{11}. \tag{11}$$

전이행렬 추정을 이용한 분포 변화 판정법은 식 (12)에 제시한 것과 같이 범주에 대한 관측도수 $f_{jk}^{(i)}$와 추정 기대도수 $\hat{E}_{jk}^{(i)}$의 차이를 이용하는 카이제곱 검정법이 사용되며, 자유도가 $(2(2-1))$인 카이제곱 분포에 근사한다는 성질을 이용한다. 즉,

$$\sum_{i=1}^{2}\sum_{j=0}^{1}\sum_{k=0}^{1}\frac{\left(f_{jk}^{(i)}-\hat{E}_{jk}^{(i)}\right)^2}{\hat{E}_{jk}^{(i)}} \sim \chi^2(2). \tag{12}$$

V. 실험적 분석

제안하는 분포 변화 탐지법의 유효성 검증 실험과 제안한 방법이 NIST의 헬스 테스트와 재시작 검정에서 검출하지 못하는 분포 변화를 탐지할 수 있는지 검증하는 실험을 진행한다. 실험은 IID로 판정된 잡음원의 분포 변화 탐지와 Non-IID로 판정된 잡음원의 분포 변화 탐지로 나누어서 진행하며, 두 분포에서 추출한 표본의 수 n_1과 n_2는 동일하게 10^6 개로 설정하였다.

실험의 정확성을 확보하기 위해 실험 데이터의 통계적 특성이 IID 또는 Non-IID임을 판정하는 과정과 재시작 검정은 NIST에서 제공하는 SP 800-90B 구현 코드[20]를 활용하였고, 제안하는 분포 판정법의 p-value 계산은 NIST에서 제공하는 SP 800-22 코드[21]를 활용하였다. 이때, 제안한 분포 판정법에서 계산된 p-value가 설정한 유의수준 α보다 작은 경우, 통계적으로 분포 변화가 발생했음을 의미한다.

5.1 IID 잡음원의 분포 변화 탐지법 검증

제안하는 IID 분포 변화 탐지법의 검증을 위해 표본 크기가 2비트인 유사균등분포(near-uniform distribution)를 실험 데이터로 사용하였다. 이때, 유사균등분포란 최대 확률을 제외한 나머지 확률이 같은 분포를 의미한다. 실험 데이터는 NIST SP 800-90B의 분포 판정에서 IID로 판정되었으며, 두 분포의 비교를 위해 분포 D_1의 최대 확률은 0.6으로 고정하였다. 실험을 통해 제안하는 분포 변화 탐지법은 IID로 판정된 잡음원의 분포 변화 탐지에 유효함을 확인할 수 있었고, 표 3을 통해 1 단계 검정보다 2 단계 검정이 엄밀하게 분포 변화를 탐지함을 확인할 수 있었다.

또한, NIST의 헬스 테스트와 재시작 검정이 검출

표 3. 제안하는 IID로 판정된 잡음원의 분포 변화 탐지법 성능 분석
Table 3. Performance of 1-step and 2-step in the proposed method for the IID noise sources

Maximum probability of D_2	1-step: Chi-square test		2-step: Two proportion test	
	p-value	$\alpha = 10^{-3}$	p-value	$\alpha = 10^{-3}$
0.6	0.6959	Non-detection	0.2835	Non-detection
0.6025	0.0013	Non-detection	0.0001	**Detection**
0.603	0.00005	**Detection**	0.00002	**Detection**

하지 못하는 엔트로피 저하가 발생하지 않은 분포 변화를 검출할 수 있는지 확인하기 위해, 2 장의 실험적 분석과 동일하게 엔트로피 저하가 발생한 경우와 엔트로피 저하가 발생하지 않은 경우로 시나리오를 설정하여 실험을 진행하였다. 실험을 통해 제안하는 분포 변화 탐지법은 NIST의 헬스 테스트와 재시작 검정과 달리, 엔트로피가 저하가 발생하지 않은 경우에도 잡음원의 분포 변화를 탐지할 수 있음을 보여주었다. 표 4는 위 실험의 결과를 요약한 것이다.

표 4. 제안하는 IID 분포 변화 탐지법과 기존 엔트로피 저하 탐지법의 성능 비교
Table 4. Comparison the proposed method with Health test and Restart test for the IID noise sources

Test / Scenario	Health test & Restart test	Proposed method	
		1-step test	2-step test
Scenario 1	Detection	Detection	Detection
Scenario 2	Non-Detection	Detection	Detection

5.2 마르코프 잡음원의 분포 변화 탐지법 검증

제안하는 마르코프 잡음원의 분포 변화 탐지법을 검증하기 위해 표본 크기가 1 비트인 1 차 마르코프 체인을 실험 데이터로 사용하였다. 두 분포의 비교를 위해 D_1 의 전이행렬은 $T_1 = \begin{pmatrix} 0.6 & 0.4 \\ 0.4 & 0.6 \end{pmatrix}$ 으로 고정하였으며, 실험 데이터는 NIST SP 800-90B의 분포 판정에서 Non-IID로 판정되었다. 표 5는 분할표 기반의 마르코프 잡음원 분포 변화 탐지법의 실험결과를 요약한 것이며, 표 6은 전이확률 추정 기반의 마르코프 잡음원 분포 변화 탐지법의 실험결과를 요약한 것이다. 실험을 통해 제안하는 두 방법은 마르코프 특성을 가지는 잡음원의 분포 변화를 유효하게 탐지함을 보여준다.

표 5. 분할표 기반의 마르코프 체인 특성의 잡음원 분포 변화 탐지법 실험 결과
Table 5. The experimental results of the contingency table-based method for the noise sources with Markov chain properties

Changing the distribution D_2	p-value	$\alpha = 10^{-3}$	$\alpha = 10^{-2}$
$T_1 = T_2$	0.5512	Non-detection	Non-detection
$T_2 = \begin{pmatrix} 0.603 & 0.397 \\ 0.4 & 0.6 \end{pmatrix}$	0.0014	Non-detection	Detection
$T_2 = \begin{pmatrix} 0.601 & 0.399 \\ 0.397 & 0.603 \end{pmatrix}$	0.0005	Detection	Detection

표 6. 전이행렬 추정 기반의 마르코프 체인 특성의 잡음원 분포 변화 탐지법 실험 결과
Table 6. The experimental results of the transition matrix estimation for the noise sources with Markov chain properties

Changing the distribution D_2	p-value	$\alpha = 10^{-3}$	$\alpha = 10^{-2}$
$T_1 = T_2$	0.3039	Non-detection	Non-detection
$T_2 = \begin{pmatrix} 0.603 & 0.397 \\ 0.4 & 0.6 \end{pmatrix}$	0.0038	Non-detection	Detection
$T_2 = \begin{pmatrix} 0.601 & 0.399 \\ 0.397 & 0.603 \end{pmatrix}$	0.0004	Detection	Detection

Ⅵ. 결 론

본 논문에서는 통계적 특성이 IID로 판정된 잡음원과 대표적인 Non-IID인 마르코프 성질을 가지는 잡음원의 분포 변화를 탐지하는 방법을 설계하였다. 제안한 방법이 IID로 판정된 잡음원과 마르코프 성질을 가지는 잡음원의 분포 변화를 효율적으로 탐지할 수 있음을 실험적으로 검증하였다. 또한, NIST의 헬스 테스트와 재시작 검정에서 검출하지 못하는 엔트로피가 저하되지 않는 경우에서도 잡음원의 분포 변화를 탐지할 수 있음을 실험적으로 확인하였다. 현재 엔트로피 추정법으로 활용되는 NIST SP 800-90B는 잡음원의 분포가 변하지 않는다는 가정에서 설계되었지만, 잡음원의 분포가 변했는지 확인하는 방법이 존재하지 않는다. 따라서, 본 논문에서 제시한 방법은 그림 4에서 제시한 것과 같이 잡음원의 분포가 기존 설계에서 변했는지 확인하는 잡음원의 정류성 검사로 활용될 것으로 기대한다. 한편, 본 논문의 연구결과는 마르코프 특성이 아닌 Non-IID 잡음원의 분포 변화 탐지법으로 활용하기 어려운 한계가 존재한다. 이에 마르코프 특성이 아닌 Non-IID 잡음원의 분포 변화 탐지법은 추후 연구로 남긴다.

References

[1] FIPS 140-2, *Security requirement for cryptographic modules*, 2001.

[2] ISO/IEC 18031: *Information technology - Security techniques - Random bit generation, International Organization for Standardization and International Electrotechnical Commission*, Second edition, 2011.

[3] E. Barker and J. Kelsey, "*Recommendation for random bit generator (RBG) construction*," NIST Special Publication 800-90C Second Draft, Apr. 2016.

[4] 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.

[5] E. Barker and J. Kelsey, "*Recommendation for Random Number Generation Using Deterministic Random Bit Generators*," NIST Special Publication 800-90A Revision 1, Jun. 2015.

[6] A. 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] W. Killmann and W. Schindler, "*Functionality classes and evaluation methodology for deterministic random number generators*," AIS.20, Sep. 1999.

[8] W. Killmann and W. Schindler, "*A Proposal for : Functionally classes and evaluation Methodology for true(physical) random number generators*," AIS.31, Sep. 2001.

[9] J. Yang, et. al., "Neural network based min-entropy estimation for random number generators," *Int. Conf. Secur. and Privacy in Commun. Syst.*, 2018.

[10] S. Zhu, et. al., "On the analysis and improvement of min-entropy estimation on time-varying data," *IEEE Trans. Info. Forensics and Secur.*, 2020.

[11] A. Bifet and R. Gavalda, "Learning from time-changing data with adaptive windowing," *SIAM Int. Conf. Data Mining*, 2007.

[12] H. Park, Y. Yeom, and J. Kang, "An analysis on the restart tests of NIST from the view point of the detection of changing distribution," in *Proc. KICS Summer Conf.*, Aug. 2020.

[13] B. Barak, R. Shaltiel, and E. Tromer, "True random number generators secure in a changing environment," in *Proc. Int. Wkshps. CHES*, Sep. 2003.

[14] A. T. Markettos and S. W. Moore, "The frequency injection attack on Ring-Oscillator-Based TRNGs," in *Proc. Int. Wkshps. CHES*, Sep. 2009.

[15] P. Bayon, et al., "Contactless electromagnetic active attack on ring oscillator based TRNG," in *Proc. Int. Wkshp COSADE*, May 2012.

[16] S. Ghandali, D. Holcomb, and C. Paar, "Temperature-based hardware Trojan for ring-oscillator-based TRNGs," *arXiv preprint arXiv:1910.00735*, 2019.

[17] A. Muthukumar, N. Sivasankari, and K. Rampriya, "Anti-aging true random number generator for secured database storage," *2017 4th Int. Conf. Advanced Comput. and Commun. Syst.*, IEEE, 2017.

[18] A. Hayter, *Probability and Statistics for Engineers and Scientists*, 4th Ed., Cengage Learning, 2012.

[19] P. Billingsley, "Statistical methods in markov chains," *The Annals of Math. Statistics*, 1961.

[20] NIST, Retrieved Feb. 21, 2021, from https://github.com/usnistgov/SP800-90B_EntropyAssessment.

[21] NIST, Retrieved Feb. 21, 2021, from https://csrc.nist.gov/Projects/Random-Bit-Generation/Documentation-and-Software.

박 호 중 (Hojoong Park)

2015년 2월 : 국민대학교 수학과 졸업
2017년 2월 : 국민대학교 금융정보보안학과 석사
2021년 2월 : 국민대학교 금융정보보안학과 박사

<관심분야> 난수성 분석, 정보보호 알고리즘 및 프로토콜, 암호이론
[ORCID:0000-0003-1179-876X]

권 수 진 (Sujin Kwon)

2020년 2월 : 국민대학교 정보보안암호수학과 졸업
2020년 3월~현재 : 국민대학교 금융정보보안학과 석사과정
<관심분야> 암호구현, 난수성 분석 및 평가, 병렬 프로그래밍
[ORCID:0000-0003-1062-6042]

염 용 진 (Yongjin Yeom)

1991년 2월 : 서울대학교 수학과 졸업
1994년 2월 : 서울대학교 수학과 석사
1999년 2월 : 서울대학교 수학과 박사

2000년 4월~2012년 2월 : ETRI 부설연구소 책임연구원/팀장
2012년 3월~현재 : 국민대학교 과학기술대학 정보보안암호수학과 정교수
2013년~현재 : 국민대학교 BK21+ 미래 금융정보보안 인력양성사업단 교수
<관심분야> 암호구현 및 분석, 보안시스템 평가
[ORCID:0000-0002-8240-8661]

강 주 성 (Ju-Sung Kang)

1989년 2월 : 고려대학교 수학과 졸업
1991년 2월 : 고려대학교 일반대학원 수학과 석사
1996년 2월 : 고려대학교 일반대학원 수학과 박사

1997년~2004년 : 한국전자통신연구원 선임연구원/팀장
2004년 3월~현재 : 국민대학교 과학기술대학 정보보안암호수학과 정교수
2013년~현재 : 국민대학교 BK21+ 미래 금융정보보안 인력양성사업단 교수
<관심분야> 암호이론, 정보보안 프로토콜, 안전성 분석 및 평가
[ORCID:0000-0002-0846-389X]