https://doi.org/10.33778/kcsa.2024.24.2.123

실난수 발생기 통계적 예측 불가능성 확인 방법

김 문 석*, 전 승 배**

요 약

사물 인터넷 시대를 맞아 700억대 이상의 다양한 기기들이 세계를 연결하고 있다. 초연결 시대로 다양한 기기들의 정보 보안은 중요한 기술 요소이다. 기밀성, 무결성, 인증 등 주요 보안 기능을 구현하기 위해 다양한 기기들의 실난수 발생기를 구현하는 것은 중요하다. 이 연구는 실난수 발생기의 난수성을 빠르게 측정하는 방법을 제안한다. 국제 표준을 통해 난수 발생기 출력의 난수성을 측정하는 방법이 있다. 하지만, 공식적인 국제 표준은 평가를 위한 많은 시간 및 비용을 소비한다. 따라서, 실난수 발생기를 구현하는 입장에서 난수성과 예측 불가능성을 빠르게 측정하는 것은 실난수 발생기를 설계하고 구현하는 입장에서 시간과 비용에 효율성을 높여준다. 첫째, 아날로그 신호의 경우 자기 상관 및 상호 상관 측정을 통해 예측 불가능성을 빠르게 측정하는 것을 제안한다. 둘째, 디지털 신호의 경우 결합 엔트로피 및 상호 정보 측정을 통해 예측 불가능성을 더 명확히 측정하는 것을 제안한다.

Methodology to Verify the Unpredictability of True Random Number Generators

Moon-Seok Kim*, Seung-Bae Jeon**

ABSTRACT

In the era of the Internet of Things, 7 billion diverse devices have been interconnected worldwide. Ensuring information security across these varied devices is crucial in this hyper-connected age. To achieve essential security functions such as confidentiality, integrity, and authentication, it is imperative to implement true random number generators (TRNGs). There fore, this study proposes a method to rapidly characterize the randomness of TRNGs. While there are international standar ds for formally characterizing the randomness of TRNGs, adhering to these standards often requires significant time and r esources. This study aims to help TRNG developers enhance efficiency in both time and cost by characterizing rough rand omness and unpredictability. Firstly, we propose applying auto-correlation and cross-correlation metrics for analog signals. Secondly, we suggest adopting joint entropy and mutual information metrics for digital signals.

Key words : True Random Number Generator(TRNG), Unpredictability, Auto correlation, Cross correlation, Markov chain, Joint entropy, Mutual information

접수일(2024년 05월 08일), 게재확정일(2024년 05월 16일)

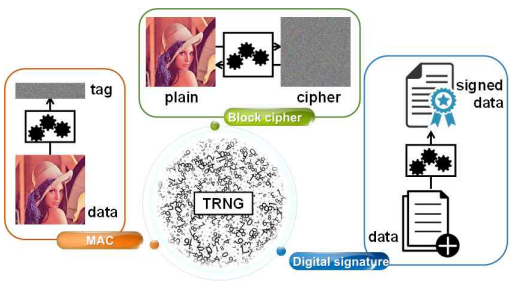
* 국립한밭대학교 반도체시스템공학과 조교수(제1저자)

** 국립한밭대학교 전자공학과 조교수(교신저자)

1. 서 론

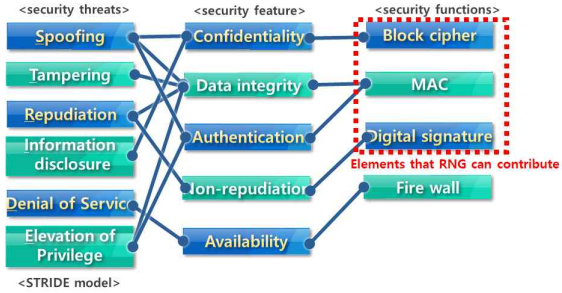
1.1 TRNG 필요성

최근 사물 인터넷(IoT: Internet of Things)이라는 새로운 컴퓨팅 패러다임이 등장하여 장치, 물건, 기계 및 사람들의 초연결성을 통해 세계를 연결할 수 있게 되었다 [1-2]. IoT 기술의 발전으로 인하여, 2025년까지 연결된 장치 수가 700억 대 이상일 것으로 전문가들은 예측하고 있다 [3-5]. 다양한 IoT 기기들의 정보 보안은 IoT 기술 보급을 위해 중요한 고려 사항이다 [6-8]. 개인 정보 보호를 달성하기 위해 각 IoT 장치는 기밀성, 무결성, 인증, 가용성 및 부인 방지라는 5가지 보안 기능을 활용해야 한다 [9-10]. 하드웨어 기반 보안 원시 중 하나인 실난수 발생기(True Random Number Generator: TRNG)는 위의 5가지 보안 기능 대부분을 지원한다 [11].



(그림 1) 주요 보안 함수들 데이터 변환 그림

첫째, 기밀성은 무단 사용자로부터 정보를 보호하는 것이다 [12]. 블록 암호는 기밀성을 달성하기 위한 전형적인 기능 중 하나이다. 기밀성의 보안 수준은 비밀 키의 엔트로피에 크게 의존한다. TRNG는 비밀 키의 엔트로피를 제공하는 소스이다. 둘째, 무결성은 정보의 출처가 전체 수명 주기 동안 진짜인지 확인하는 것이다. 셋째, 인증은 사용자가 승인된 사용자인지 확인하는 보안 프로세스이다 [12]. 메시지 인증 코드(Message Authentication Code: MAC)는 무결성과 인증을 보장하는 전형적인 기능 중 하나이다 [13]. MAC 함수는 또한 TRNG로부터의 엔트로피 소스를 동반한 비밀 키를 요구한다. 넷째, 가용성은 정보가 승인된 사용자에게 접근 가능한 것이다 [14]. 다섯째, 부인 방지는 데이터의 출처와 데이터의 무결성을 증명하는 서비스이다. 데이터의 출처 증명은 확인자가 정보의 발신자를 확인할 수 있다는 것을 의미한다. 디지털 서명은 부인 방지를 달성하기 위한 전형적인 기능이다. 디지털 서명의 보안 수준을 보장하기 위해서는 비공개 키와 공개 키 쌍의 엔트로피를 보장하는 것이 중요하다. (그림 1)은 블록 암호, MAC 함수, 디지털 서명의 입력 및 출력 데이터 변환을 시각적으로 표현해 준다. 블록 암호는 평문을 암호문으로 변환하는 함수이고, MAC 함수는 데이터로부터 태그 보안 정보를 생성하는 함수이다. 마지막으로, 디지털 서명은 전자 데이터 생산자가 누구인지 서명할 수 있는 기능을 제공한다.



(그림 2) 보안 위협- 보안 기능- 보안 함수 연결 그림

(그림 2)은 보안 위협 대응을 위한 보안 기능, 그리고 보안 기능을 구현해주는 보안 함수들을 보여준다. 이중 TRNG는 블록 암호, MAC, 디지털 전자 서명 보안 함수 구현에 직접적으로 기여한다. TRNG는 비공개 키와 공개 키 쌍을 생성하는 엔트로피 소스이다. 5가지 독특한 특징 중에서 TRNG는 기밀성, 무결성, 인증 및 부인 방지를 지원하는 데 기여한다. 이러한 이유로 각 IoT 장치에 실난수 발생기를 구현하는 것이 중요하다. 이 논문에서는 이 구현한 실난수 발생기의 평가 방법을 제안한다. 국제 표준을 통하여 실난수 발생기의 예측 불가능성 및 난수성을 평가하는 방법들이 있다. 하지만, 국제 표준을 적용한 난수성 평가는 엄격한 평가 방법으로 인한 평가를 위한 많은 시간 및 자원이 필요한 단점이 있다. 따라서, 이 논문에서는 TRNG를 구현하는 입장에서 아날로그 신호와 디지털 신호로 나누어 빠르게 평가하

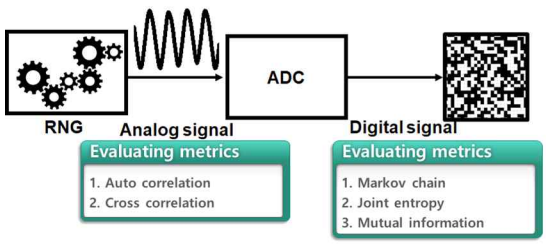
는 방법들을 제안한다. 이 연구를 통하여 구현한 난수 발생기의 예측 불가능성을 간단히 예측할 수 있는 방법을 제안한다.

1.2 TRNG 평가 지표 동향

난수 발생기는 미국 NIST(National Institute of Standards and Technology)에서 제정한 국제 표준이 존재한다. NIST SP800-22 표준은 난수 발생기가 생성한 디지털 난수 결과물을 통계적으로 분석하여 난수성을 확인하는 표준이다 [15]. 이미 생성한 난수들의 통계적 검사만 수행하는 NIST SP800-22 표준을 보완하기 위한 목적으로 NIST SP800-90 표준이 있다 [16]. NIST SP800-90 표준은 난수 발생기가 지속적으로 안전한 엔트로피를 제공하기 위한 방법과 절차를 정의한다. TRNG의 적절성을 엄격히 확인하기 위해서, 이 두 국제 표준을 적용하는 것은 적합하다. 하지만, 이 두 표준은 난수 발생기의 적절성을 확인하기 위해 많은 평가 지표들과 평가 시간이 필요한 단점이 있다. 따라서, TRNG를 구현하는 입장에서는 구현한 난수 발생기를 엄격하게 평가하기 전에 빠르게 평가하기 위한 평가 지표들이 필요하다.

2. TRNG 특성 평가 지표 목록

이 논문에서는 평가 지표를 아날로그 신호 특성 평가 방법과 디지털 신호 특성 평가 방법으로 구분한다. (그림 3)은 아날로그 신호와 디지털 신호 각각 제안하는 평가지표 목록을 보여준다. TRNG의 경우 아날로그 신호를 디지털 신호로 변환하여 난수 발생기의 결과물로 활용하는 경우가 많다. 따라서, 디지털 신호로 변환하기 전에 더욱 빠르게 신호의 예측 불가능성을 확인하는 평가 지표를 제안한다. 제안하는 평가 지표는 자기 상관, 상호 상관 지표가 있다. 또한, 생성한 디지털 신호를 이용하여 TRNG로서의 예측 불가능성을 측정하는 지표를 제안한다. 디지털 신호 평가 지표는 마르코프 체인, 결합 엔트로피, 상호 정보 지표가 있다.



(그림 3) TRNG 특성평가 지표 목록

3. 아날로그 신호 특성 평가

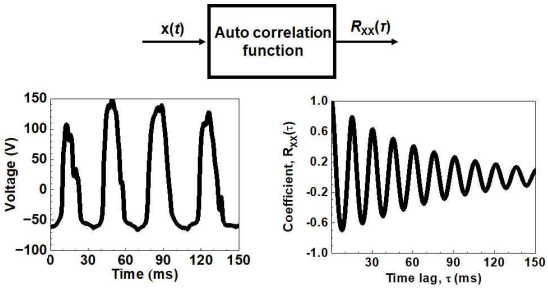
3.1 자기 상관

자기 상관은 -1.0 ~ +1.0 범위의 실수로 나타나는 함수이다. 자기 상관 함수는 하나의 신호가 시간 변화에 따른 상관 관계를 정량적으로 보여준다 [17-18]. 0에 가까울수록 동일한 변수의 서로 다른 시간에서의 두 값 사이의 자기 상관이 적다는 뜻이다. 다시 한번 정리하면, 자기 상관 계수는 하나의 장치 내 신호의 시간 변화에 따른 유사성을 측정할 수 있는데, 이는 단일 신호의 시간 지연에 따른 자기 유사성을 나타낸다 [19-20]. 자기 상관 함수를 이용하여 장치 내부(intra-device)에서의 시간 변화에 따른 예측 불가능성을 측정이 가능하며, 상호 상관 함수를 통해 장치 간(inter-device)의 예측 불가능성을 측정할 수 있다. 자기 상관 함수는 아래 수식으로 계산할 수 있다.

$$R_{XX}(\tau) = \frac{1}{|R_{XX}(0)|^2} \int_{-\infty}^{+\infty} x(t)x(t+\tau)dt$$

모든 계수는 시간 지연이 없는 경우에 대한 계수인 $|R_{XX}(0)|^2$로 정규화한다. 따라서, 정규화된 자기 상관 함수의 정의에 따라 $R_{XX}(0)$의 자기 상관 계수는 항상 1이다. -1의 상관은 완전한 음의 상관을 나타내고, 1의 상관은 완전한 양의 상관을 나타낸다. 그에 반해, 0의 상관은 서로 다른 시간에 동일한 변수 간의 선형 관계가 없음을 의미한다 [21-22]. 이는 테스트 신호가 시간 변화에 따라 다음 신호가 예측 불가능함을 뜻한다. (그림 4)는 자기 상관 함수의 입력에 따른 출력 예시를 보

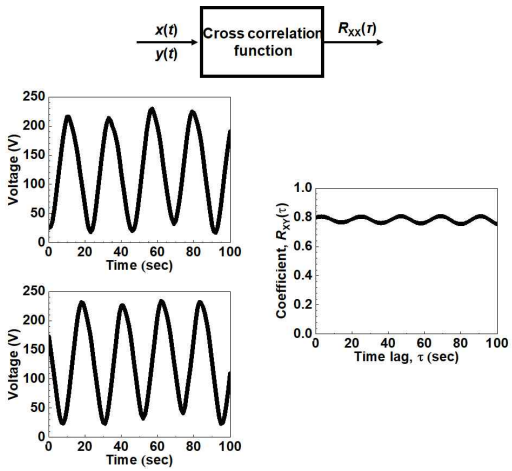
여준다. 자기 상관 함수의 필요한 입력은 시간에 따른 단일 장치에 출력 결과이다. 예시에서는 시간에 따른 전압 변화 그림을 보여준다. 자기 상관 함수는 이 입력 신호가 시간 변화에 따른 신호 전체의 상관도를 -1.0 ~ 1.0 범위의 실수로 보여준다. (그림 4)의 예시 출력 그림은 상관도가 시간 변화에 따라 줄어드는 경향성을 보여준다. 즉, (그림 4) 왼쪽의 $x(t)$ 신호는 150ms 시간이 지나면 자기 상관도가 0.0에 수렴하는 신호가 됨을 뜻한다. 이는 구현한 단일 난수 발생기가 150 ms 이상 시간 차이가 나는 신호는 서로 예측 불가능한 특성을 보이고, 반대로 150 ms 이내의 시간 차이에서는 출력한 신호가 통계적으로 상관도가 있다는 것을 뜻한다.



(그림 4) 자기 상관 함수 계산 예시

3.2 상호 상관

상호 상관은 -1.0 ~ +1.0 범위의 실수로 나타나는 함수이다. 상호 상관 함수는 두 개의 신호의 시간 변화에 따른 상관 관계를 정량적으로 보여준다 [23-24]. 값이 0에 가까울수록 두 개의 신호 사이의 상관 관계가 적다는 것을 뜻한다 [21-22]. 즉, 자기 상관은 하나의 TRNG 장치의 시간 변화에 따른 상관 관계를 측정하는 지표라면, 상호 상관은 두 개의 TRNG 장치의 상관 관계를 측정할 수 있는 지표이다. (그림 5)는 상호 상관 함수의 입력에 따른 출력 예시를 보여준다. 상호 상관 함수는 2 개의 시간에 따른 출력이 필요하다. 상호 상관은 두 입력 신호의 시간 변화에 따른 신호 전체의 상관도를 -1.0 ~ 1.0 범위의 실수로 보여준다. (그림 5)의 예시 출력 그림은 상호 상관도가 시간 변화에 따라 주기적으로 변하지만 전체적인 상관도는 100초가 지나도 줄어들지 않는 경향성을 가진다. 즉, $x(t)$, $y(t)$ 두 입력은 시간의 관계없이 높은 상관도를 보이는 신호임을 알 수 있다. 하나의 TRNG 장치의 출력을 알면 다른 TRNG 장치의 출력도 통계적으로 예측 가능함을 뜻한다. 장치 간 상호 상관 계수 계산은 아래와 같이 수행한다.



(그림 5) 상호 상관 함수 계산 예시

$$R_{XY}(\tau) = \frac{1}{|R_{XX}(0)||R_{YY}(0)|}\int_{-\infty}^{+\infty} x(t)y(t+\tau)dt$$

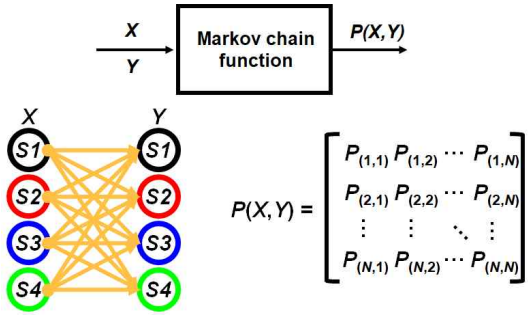
3장에서는 TRNG에서 생성하는 아날로그 신호의 예측 불가능성을 시각적/정량적으로 평가하는 방법을 살펴보았다. 자기 상관, 상호 상관 두 평가 지표 모두 아날로그 신호를 간단한 계산으로 예측 불가능성을 빠르게 평가할 수 있는 지표이다. 자기 상관은 하나의 TRNG 인트라 디바이스의 예측 불가능성을 측정하기 좋은 평가 지표이다. 반면에, 상호 상관은 두 개 이상의 TRNG 인터 디바이스의 예측 불가능성을 측정하기 좋은 평가 지표이다.

4. 디지털 신호 특성 평가

4.1 마르코프 체인

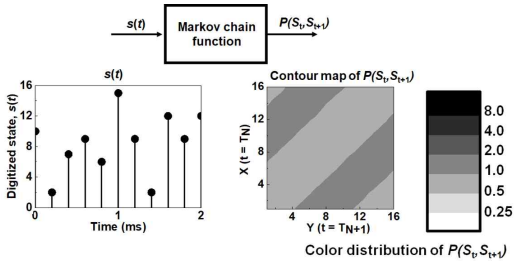
4장은 TRNG에서 생성한 최종 결과물인 디지털 비트들의 통계적 예측 불가능성을 평가

할 수 있는 지표들을 소개한다. 첫 번째로, 마르코프 체인은 간단한 행렬 계산을 통해 불확실성과 예측 불가능성을 분석하는 방법이다 [25-27]. 특히, 마르코프 체인 모델 계산 결과를 통해 결합 엔트로피와 상호 정보의 값을 계산하여 예측 불가능성을 정량적으로 평가할 수 있다. (그림 6)은 디지털 신호 입력을 행렬로 변환하는 것을 간단하게 보여준다. 예를 들어, TRNG가 2비트를 한번에 생산한다고 가정하면, 생산한 2비트는 4개의 상태(state) 정의할 수 있다. 그리고 다음 샘플링 시간 때 생산한 2비트로 4개의 상태로 재설정 할 수 있다.



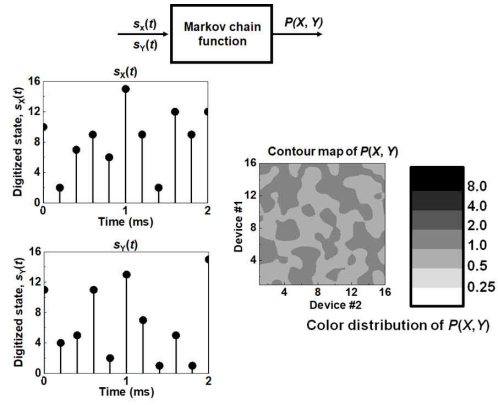
(그림 6) 디지털 신호 상태 변화 행렬 계산 그림

처음 4개의 상태를 랜덤 변수 X, 다음 4개의 상태를 랜덤 변수 Y라고 정의할 수 있다. 마르코프 체인은 랜덤 변수 X와 Y로의 상태 변화를 확률 분포를 행렬로 표현한 것이다. 시간 변화에 따른 확률 분포 표현은 인트라 장치 마르코프 체인이라고 한다 [28-29]. (그림 7)은 인트라 장치의 마르코프 체인 계산 예시를 보여준다. 입력 신호인 $s(t)$ 신호는 단일 TRNG 장치의 시간에 따른 상태 변화를 보여준다. 전체 상태 수는 16개이다.



(그림 7) 인트라 장비 마르코프 체인 행렬 계산 예시

$s(t)$ 신호의 확률 분포를 계산한 것이 $P(S_t, S_{t+1})$ 이고 (그림 7)에서 확률 밀도를 등고선 그림으로 변환하여 보여주고 있다. 즉, 인트라 장비 마르코프 체인 $P(1, 1)$은 상태 1에서 상태 1로 상태 변화가 일어나는 확률 밀도 크기를 보여준다. (그림 8)은 인터 장치의 마르코프 체인 계산 예시를 보여준다. 입력 신호인 $s_X(t)$, $s_Y(t)$ 신호는 복수 TRNG 장치의 시간에 따른 상태 변화를 보여준다. 동일한 시간 $s_X(t)$, $s_Y(t)$ 신호 간의 상태 차이를 확률 분포로 계산한 것이 $P(X, Y)$ 이고 (그림 8)에서 등고선 그림으로 보여주고 있다. (그림 8)에서 설명하는 인터 장비 마르코프 체인 $P(1, 1)$은 장치#1과 장치#2의 상태가 모두 상태 1인 확률 밀도를 보여준다. 아날로그-디지털 변환기(ADC: Analog Digital Converter)로부터 추출한 비트의 크기가 n이라고 하면, 마로크코프 체인 행렬은 $2^n \times 2^n$ 크기의 행렬을 가진다 [30-31].

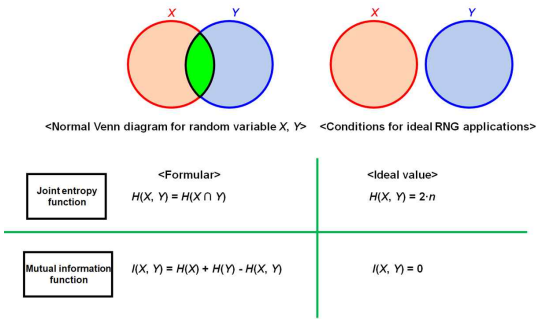


(그림 8) 인터 장비 마르코프 체인 행렬 계산 예시

4.2 결합 엔트로피

앞에 절에서 설명한 마르코프 체인 행렬을 등고선으로 그림화하여 확률 밀도를 통해 예측 불가능성을 확인할 수 있다. 제안하는 결합 엔트로피와 상호 정보는 앞에 절에서 계산한 확률 밀도를 이용하여 측정할 수 있다 [32-35]. (그림 9)는 결합 엔트로피와 상호 정보의 의미를 벤 다이어그램과 수식으로 표현해 준다. 두 랜덤 변수 X와 Y가 있다고 할 때 TRNG가 생성하는 정보들은 두 랜덤 변수 간의 교집합이 없어야 하나의 랜덤 변수로부터 다른 랜덤 변수가 예측 불가능하다. 결합 엔트로피는 두 랜덤 변수 X와 Y에 엔트로피가

유지되어야 한다. 정리하자면, ADC로부터 n비트 출력을 하는 TRNG의 엔트로피는 n이어야 하며, 두 랜덤 변수 X와 Y의 결합 엔트로피의 이상값은 $2{\cdot}n$이다. (그림 10)은 마르코프 체인 행렬 확률 밀도로부터 결합 엔트로피 출력 결과를 알 수 있는 것을 보여준다. 확률 밀도 함수로부터 결합 엔트로피 계산 수식을 아래와 같다.



(그림 9) 결합 엔트로피 및 결합 정보의 벤 다이어그램 의미 및 수식

$$P(X,Y)=\begin{bmatrix} P_{(1,1)} & \cdots & P_{(1,N)} \\ \vdots & \ddots & \vdots \\ P_{(N,1)} & \cdots & P_{(N,N)} \end{bmatrix}$$

$$P(X)=[P_1,\ \cdots P_j \cdots, P_N],\ where\ P_j=\sum_{l=1}^{N} P_{(j,l)}$$

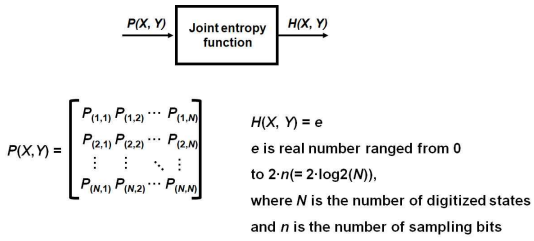
$$P(Y)=[P_1,\ \cdots P_k \cdots, P_N],\ where\ P_k=\sum_{m=1}^{N} P_{(k,m)}$$

모든 구성 요소의 합은 1이다, 즉, 아래 수식을 만족한다.

$$\sum_{k=1}^{N}\sum_{j=1}^{N} P_{(j,k)}=1$$

수식을 정리하면 결합 엔트로피는 $P(X,Y) = P(X){\cdot}P(Y)$를 확인하여 불확실성을 측정한다 [36-37]. 계산한 마르코프 체인 행렬로부터 결합 엔트로피 계산하는 구체적인 수식은 아래와 같다. 이 때 상호 엔트로피는 인트라 장비, 인터 장비 모두 측정 가능하다.

$$H(X,Y)=-\sum_{j=1}^{N}\sum_{k=1}^{N} P_{(j,k)}\ \cdot\ \log_2 P_{(j,k)}$$



(그림 10) 결합 엔트로피 입출력 함수

4.2 상호 정보

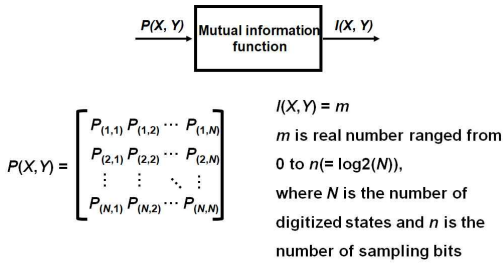
상호 정보 $I(X, Y)$는 불확실성을 설명하는 또 다른 지표이다 [38-39]. 아래 수식과 같이 간단히 계산 가능하다.

$$I(X,Y)=H(X)+H(Y)-H(X,Y)$$

$$H(X)=-\sum_{j=1}^{N} P_j\ \cdot\ \log_2 P_j,\ where\ P_j=\sum_{l=1}^{N} P_{(j,l)}$$

$$H(Y)=-\sum_{k=1}^{N} P_k\ \cdot\ \log_2 P_k,\ where\ P_k=\sum_{m=1}^{N} P_{(m,k)}$$

(그림 11)은 마르코프 체인 행렬 확률 밀도로부터 상호 정보 출력 결과를 알 수 있는 것을 보여준다. 작은 상호 정보 출력은 두 랜덤 변수 X와 Y가 예측할 수 없다는 것을 나타낸다 [56-57]. 인트라 장비 상호 정보 측정의 경우, 같은 장치 내 시간 변화에 따른 상호 정보를 양적으로 측정한다. 인트라 장비 $I(X, Y) = 0$의 이상적인 결과는 시간 변화에 관계 없이 예측 불가능 특징을 가진다는 것을 의미한다 [40-41]. 인터 장비 상호 정보 측정의 경우, 다른 장치 간의 상호 정보를 양적으로 측정할 수 있다. 인터 장비 $I(X, Y) = 0$의 이상적인 결과는 장치 #1의 난수 결과를 알더라도, 장치 #2의 출력이 예측 불가능하다는 것을 뜻한다 [42-43].



(그림 11) 상호 정보 입출력 함수

6. 결론

구현한 실난수 발생기의 난수성과 예측 불가능성을 정량적으로 검증하기 위한 방법들을 제안하였다. 먼저, 아날로그 신호를 통해 실난수 발생기의 출력을 디지털 신호로 변경하기 전에 예측 불가능성을 확인하는 방법을 제안하였다. 이는 자기 상관 함수를 이용하여 장치 내부(intra-device)에서의 시간 변화에 따른 예측 불가능성을 측정하는 것으로 가능하며, 또한 상호 상관 함수를 통해 장치 간(inter-device)의 예측 불가능성을 측정할 수 있다. 다음으로, 실난수 발생기의 최종 디지털 출력 신호를 통해 예측 불가능성을 확인하는 방법을 제안하였다. 이는 결합 엔트로피와 상호 정보 측정을 활용하여 단일 장치(intra-device) 및 장치 간(inter-device)의 통계적 예측 불가능성을 확인하는 것을 포함한다.

참고문헌

[1] H. N. Saha, A. Mandal, and A. Sinha, Recent trends in the Internet of Things, *2017 IEEE 7th annual computing and communication workshop and conference (CCWC)*. (2017) 1-4.

[2] M. H. Alsharif, A. H. Kelechi, S. Kim, I. Khan, J. Kim, and J. H. Kim, Enabling hardware green internet of things: a review of substantial issues, *IEEE Access*. (2019) 1-21.

[3] K. Rose, S. Eldridge, and L. Chapin, The internet of things: An overview, *The Internet Society (ISOC)*. 80 (2015) 1-50.

[4] E. P. Yadav, E. A. Mittal, and H. Yadav, IoT: Challenges and issues in indian perspective, *2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU)*. (2018) 1-5.

[5] B. Ji, K. Song, C. Li, W. P. Zhu, and L. Yang, Energy harvest and information transmission design in internet-of-things wireless communication systems, *AEU-International Journal of Electronics and Communications*. 87 (2018) 124-127.

[6] T. J. Charity, and H. J. Hua, Smart world of internet of things (IoT) and its security concerns, *2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. (2018) 240-245.

[7] Q. Huang, Y. Yang, and L. Wang, Secure data access control with ciphertext update and computation outsourcing in fog computing for Internet of Things, *IEEE Access*. 5 (2017) 12941-12950.

[8] H. Yan, X. Li, Y. Wang, and C. Jia, Centralized duplicate removal video storage system with privacy preservation in IoT, *Sensors*. 18 (2018) 1814.

[9] C. L. Chen, Y. Y. Deng, W. Weng, C. H. Chen, Y. J. Chiu, and C. M. Wu, A traceable and privacy-preserving authentication for UAV communication control system, *Electronics*. 9 (2020) 62.

[10] Z. E. Mrabet, N. Kaabouch, H. E. Ghazim and H. E. Ghazi, Cyber-security in smart grid: Survey and challenges, Computers & Electrical Engineering. 67 (2016) 1-4.

[11] M. S. Kim, I. W. Tcho, and Y. K. Choi, Analyses of unpredictable properties of a wind-driven triboelectric random number

generator, Scientific Reports. 13 (2023) 16610.

[12] S. Sicari, A. Rizzardi, and A. C. Porisini, 5G in the Internet of Things era: an overview on security and privacy challenges, Computer Networks. 179 (2020) 107345.

[13] G. K. Sodhi, G. S. Gaba, L. Kansal, and E. Babulak, Preserving Authenticity and Integrity of Distributed Networks through Novel Message Authentication Code, Indonesian Journal of Electrical Engineering and Computer Science. 12 (2018) 1297-1304.

[14] M. Malekzadeh, A. A. A. Ghani, and S. Subramaniam, A new security model to prevent denial of service attacks and violation of availability in wireless networks, International Journal of Communication Systems. 25 (2012) 903-925.

[15] Luengo, E. A., Olivares, B. A., Villalba, L. J. G., & Hernandez-Castro, J,. Further analysis of the statistical independence of the NIST SP 800-22 randomness tests, Applied Mathematics and Computation. 459 (2023) 128222.

[16] Buller, D., Kaufer, A., Roginsky, A., and Turan, M. S., Discussion on the Full Entropy Assumption of the SP 800-90 Series, (2023).

[17] B. J. Berne, J. P. Boon, and S. A. Rice, On the calculation of autocorrelation functions of dynamical variables, The Journal of Chemical Physics. 45 (1966) 1086-1096.

[18] X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H. K. Lo, Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction, Physical Review A. 87 (2013) 062327.

[19] V. Carruba, S. Aljbaae, R. C. Domingos, M. Huaman, and W. Barletta, Chaos identification through the autocorrelation function indicator, Celestial Mechanics and Dynamical Astronomy. 133 (2021) 38.

[20] H. Wu, J. Xu, J. Wang, and M. Long, Autoformer: Decomposition transformers with auto-correlation for long-term series forecasting, Advances in Neural Information Processing Systems. 34 (2021).

[21] B. H. Baltagi, S. H. Song, B. C. Jung, and W. Koh, Testing for serial correlation, spatial autocorrelation and random effects using panel data, Journal of econometrics. 140 (2007) 5-51.

[22] F. Diaz, Performance prediction using spatial autocorrelation, Proceedings of the 30th annual international ACM SIGIR conference on Research and development in information retrieval. (2007) 583-590.

[23] E. S. Lohan, Statistical analysis of BPSK-like techniques for the acquisition of Galileo signals, Journal of Aerospace Computing, Information, and Communication. 3 (2006) 234-243.

[24] G. F. Zebende, DCCA cross-correlation coefficient: Quantifying level of cross-correlation, Physica A: Statistical Mechanics and its Applications. 390 (2011) 614-618.

[25] K. Plenkers, J. R. R. Ritter, and M. Schindler, Low signal-to-noise event detection based on waveform stacking and cross-correlation: Application to a stimulation experiment, Journal of seismology. 17 (2013) 27-49.

[26] M. Kafsi, M. Grossglauser, and P. Thiran, The entropy of conditional Markov trajectories. IEEE Transactions on Information Theory. 59 (2013) 5577-5583.

[27] M. C. Choi, Velocity formulae between entropy and hitting time for Markov

chains, Statistics & Probability Letters. 141 (2018) 62-67.

[28] L. Ricci, Asymptotic distribution of sample Shannon entropy in the case of an underlying finite, regular Markov chain, Physical Review E. 103 (2021) 022215.

[29] S. Chakraborty, Generating discrete analogues of continuous probability distributions-A survey of methods and constructions, Journal of Statistical Distributions and Applications. 2 (2015) 1-30.

[30] M. Hajar, M. El Badaoui, A. Raad, and F. Bonnardot, Discrete random sampling: Theory and practice in machine monitoring, Mechanical Systems and Signal Processing. 123 (2019) 386-402.

[31] M. Kim, U. Ha, K. J. Lee, Y. Lee, and H. J. Yoo, A 82-nW chaotic map true random number generator based on a sub-ranging SAR ADC, IEEE Journal of Solid-State Circuits. 52 (2017) 1953-1965.

[32] F. Özkaynak, Cryptographically secure random number generator with chaotic additional input, Nonlinear Dynamicsi. 78 (2014) 2015-2020.

[33] L. Gong, J. Zhang, L. Sang, H. Liu, and Y. Wang, The Unpredictability Analysis of Boolean Chaos, IEEE Transactions on Circuits and Systems II: Express Briefs. 67 (2019) 1854-1858.

[34] M. Inubushi, Unpredictability and robustness of chaotic dynamics for physical random number generation, Chaos: An Interdisciplinary Journal of Nonlinear Science. 29 (2019) 033133.

[35] J. A. Karell-Albo, C. M. Legon-Perez, E. J. Madarro-Capo, O. Rojas, and G. Sosa-Gomez, Measuring independence between statistical randomness tests by mutual information, Entropy. 22 (2020) 741.

[36] S. J. Barigye, Y. Marrero Ponce, Y. Martínez López, F. Torrens, L. M. Artiles Martínez, R. W. Pino Urias, and O. Martínez Santiago, Relations frequency hypermatrices in mutual, conditional, and joint entropy based information indices, Journal of Computational Chemistry. 34 (2013) 259-274.

[37] M. Madiman, and P. Tetali, Information inequalities for joint distributions, with interpretations and applications, IEEE Transactions on Information Theory. 56 (2010) 2699-2713.

[38] X. Ma, X. Huang, S. Du, H. Liu, and X. Ning, Symbolic joint entropy reveals the coupling of various brain regions, Physica A: Statistical Mechanics and its Applications. 490 (2018) 1087-1095.

[39] L. Chen, V. P. Singh, and S. Guo, Measure of correlation between river flows using the copula-entropy method, Journal of Hydrologic Engineering. 18 (2013) 1591-1606.

[40] D. Marco, and D. L. Neuhoff, Entropy of highly correlated quantized data, IEEE Transactions on Information Theory. 56 (2010) 2455-2478.

[41] Y. S. Kim, Y. Yeom, and H. B. Choi, Online test based on mutual information for true random number generators, Journal of the Korean Mathematical Society. 50 (2013) 879-897.

[42] A. Namdari, and Z. Li, A review of entropy measures for uncertainty quantification of stochastic processes, Advances in Mechanical Engineering. 11 (2019) 1687814019857350.

[43] M. Eskafi, M. Kowsari, A. Dastgheib, G. F. Ulfarsson, P. Taneja, and R. I. Thorarinsdottir, Mutual information anal-

ysis of the factors influencing port throughput, Maritime Business Review. 6 (2020) 129-146.

[44] J. P. Pluim, J. A. Maintz, and M. A. Viergever, Mutual-information-based registration of medical images: a survey, IEEE transactions on medical imaging. 22 (2003) 986-1004.

〔저 자 소 개〕

김 문 석 (Moon-Seok Kim)
2011년 2월 중앙대학교 학사
2013년 2월 한국과학기술원 석사
2022년 2월 한국과학기술원 박사
2023년 9월~현재: 국립한밭대학교 반도체시스템공학과 조교수
email : mskim@hanbat.ac.kr

전 승 배 (Seung-Bae Jeon)
2013년 2월 한국과학기술원 학사
2015년 2월 한국과학기술원 석사
2019년 2월 한국과학기술원 박사
2021년 9월~현재: 국립한밭대학교 전자공학과 조교수
email : sbjeon@hanbat.ac.kr