분포 변화 탐지 관점의 NIST 재시작 검정 분석

박호중[2], 염용진[1,2], 강주성† [1,2]

국민대학교 정보보안암호수학과[1] / 금융정보보안학과[2]

{ruokay, salt, jskang† }@kookmin.ac.kr

An Analysis on the Restart tests of NIST from the view point of the Detection of Changing Distribution

Hojoong Park, Yongjin Yeom, Ju-Sung Kang†

Dept. of Information Security, Cryptology, and Mathematics [1]/
Financial information security [2], Kookmin Univ.

요 약

난수발생기의 엔트로피 추정법으로 활용되는 NIST의 SP 800-90B는 잡음원의 분포가 변하지 않는다는 가정에서 설계되었다. 하지만, 실제 사용 환경에서 난수발생기는 탑재 상태의 변화, 노후 현상의 발생 등과 같이 잡음원의 수집 환경 변화로 인한 출력수열의 분포가 변하는 현상이 발생할 수 있다. 본 논문에서는 기존에 진행되지 않았던 분포 변화 탐지 관점에서 NIST의 재시작 검정을 분석하여 그 의의와 한계점을 확인한다.

Ⅰ. 서 론

안전한 암호통신 시스템을 설계하기 위해서는 안전성이 검증된 암호학적 난수발생기의 사용이 필수적이다. 이전 암호학적 난수발생기의 안전성은 구성 알고리즘의 구조적인 안전성과 최종 출력 난수의 통계적 난수성을 중심으로 평가가 진행되었다. 하지만, 난수발생기의 본질적인 안전성은 입력의 예측 불가능성에 달려있기 때문에, 현재는 난수발생기의 입력으로 수집되는 잡음원(Noise source)의 예측 불가능성 측정이 안전성 평가에 중요한 요소로 자리잡고 있다. 미국 NIST의 SP 800-90B는 대표적인 엔트로피 평가 방법으로 현재 암호모듈검증제도(Cryptographic Module Validation Program, CMVP)에서 활용되고 있다. NIST SP 800-90B에 제시된 평가 방법은 잡음원의 예측 불가능성을 보수적으로 추정하기 위해 최소엔트로피(min-entropy)를 측도로 사용하며, 이는 공격자의 최적 예측 공격(optimum guessing attack)과 관계가 있음이 알려져 있다[1, 2].

NIST SP 800-90B에서는 잡음원이 시간이 지나도 분포가 변하지 않는 정류적(Stationary) 성질을 만족하도록 권고하고 있으며, SP 800-90B의 엔트로피 추정은 잡음원의 분포를 가정하지 않고, 잡음원 출력 수열만으로 엔트로피를 추정하는 블랙박스(Black-box) 방식을 채택하고 있다. 그렇기 때문에, SP 800-90B의 엔트로피 추정은 수집한 잡음원 분포의 I.I.D.(Independent and identically distributed) 여부를 먼저 판정(Determine the track)한 후, 엔트로피를 추정(Estimate entropy)하는 순서로 진행된다. 잡음원의 엔트로피 추정은 분포의 I.I.D. 판정 결과에 기반하여 IID track과 Non-IID track으로 나누어져 진행된다. 엔트로피 추정이 완료된 후에는 난수발생기의 동작을 켜고 끄는 것을 반복하여 잡음원을 수집하여 잡음원 출력 간 상관관계 존재 여부 등을 확인하는 재시작 검정(Restart test)을 진행하고, 컨디셔닝(Conditioning component)의 사용 여부에 맞추어 잡음원의 최종 엔트로피 추정치를 출력한다.

한편, 잡음원의 정류적 특성을 만족시키기 위해서는 난수발생기 탑재 상태의 변화, 노후 현상(aging effect) 등이 발생하지 않는 것과 같이 잡음원의 수집 환경이 안정적이어야 한다. 하지만, 실제 암호통신 시스템에서 위 현상들이 발생할 수 있다. 이에 본 논문에서는 시간이 지남에 따라 잡음원의 분포가 변하는 현상을 탐지하는 관점으로 재시작 검정을 분석한다. 우리의 실험적 분석 결과에 의하면, SP 800-90B 내에서 행하는 재시작 검정은 분포의 변화를 완전히 탐지하지는 못 하지만, 가정된 엔트로피보다 저하되어 분포가 유지되지 않는 경우는 탐지 가능함을 확인할 수 있었다.

Ⅱ. NIST의 재시작 검정

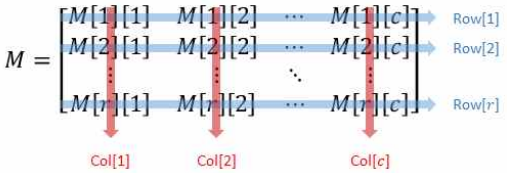
2.1 재시작 검정의 개요

NIST의 재시작 검정(Restart test)은 이전에 출력된 잡음원과 나중에 출력된 잡음원 사이에 연관성이 존재하여, 추정된 엔트로피보다 다음에 출력될 잡음원의 예측 가능성이 높아지는 취약점을 검출하기 위한 목적으로 설계되었다. 재시작 검정은 건전성 검사(Sanity check)와 엔트로피 갱신의 두 단계로 구성된다. 재시작 검정의 가장 큰 특징은 난수발생기의 전원을 켜고 끄는 행위를 반복하여 재시작 검정용 잡음원을 새로 수집하고, 이 잡음원의 엔트로피 추정치와 기존 잡음원의 엔트로피 추정치를 비교하여 엔트로피를 갱신하는 순서로 진행된다.

2.2 NIST의 재시작 검정

1) 재시작 검정의 건전성 검사 단계

재시작 횟수를 r이라 할 때, 재시작 시점마다 c 개의 샘플을 수집하여 구성한 재시작 검정용 데이터는 [그림 1]과 같이 행렬 M으로 표현한다.



[그림 1] 재시작 검정용 데이터 구성

NIST의 재시작 검정에서는 c와 r을 1,000으로 설정하고 있으며, 이는 재시작 검정용 데이터는 재시작 한 번에 1,000개의 잡음원 샘플을 수집하고 1,000번 반복하여 수집함을 의미한다. 즉, 재시작 검정은 난수발생기 재시

† Corresponding Author

작을 반복하여 수집한 10^6개의 잡음원 샘플로 진행된다.

건전성 검사는 [알고리즘 1]과 같이 재시작 검정 직전에 추정된 엔트로피 H_I보다 행렬 M의 각 행과 열에서 발생하는 잡음원 샘플 값의 최대 빈도가 많이 발생하는지 확인하여, 많이 발생한 경우 탈락으로 판정한다. 가장 많이 발생한 샘플 값의 수를 확률변수 X라 하면, X는 크기가 1,000이고, 성공확률이 $p=2^{-H_I}$인 이항분포를 따른다. 즉, $X \sim B(1000, p)$. 한편, 건전성 검사는 그 설계를 분석했을 때, 재시작으로 인해 발생하는 분포 유지 실패를 검출하기 위해 설계된 것으로 보인다.

[알고리즘 1] 재시작 검정에 사용되는 건전성 검사

알고리즘: 건전성 검사

1: $p=2^{-H_I}$, $\alpha=0.000005$로 설정.

2: 각 행과 열에서 가장 많이 발생한 샘플의 수 $x_{\max}$를 계산

3: $P(X \geq x_{\max}) = \sum_{j=x_{\max}}^{1000} \binom{1000}{j} p^j (1-p)^{1000-j}$을 계산

4: $P(X \geq x_{\max}) < \alpha$이면, 실패

2) 재시작 검정의 엔트로피 갱신 단계

$1 \leq i \leq 1000$인 i에 대해, i 번째 재시작에서 수집된 데이터인 $Row[i]$는 $Row[i]=M[i][1] \| M[i][2] \| \cdots \| M[i][c]$이고, 각 재시작에서 i 번째로 수집된 데이터인 $Col[i]$는 $Col[i]=M[1][i] \| M[2][i] \| \cdots \| M[c][i]$이라 하자. 엔트로피 갱신 단계에서는 [그림 1]과 같이 잡음원을 행 데이터 S_r과 열 데이터 S_c로 재구성한 후, S_r과 S_c 각각에 대해 엔트로피를 추정한다. S_r과 S_c는 각각 $S_r = Row[1] \| Row[2] \| \cdots \| Row[r]$과 $S_c = Col[1] \| Col[2] \| \cdots \| Col[c]$와 같이 구성된다. 기존 잡음원의 I.I.D. 판정 여부에 맞추어 S_r과 S_c의 엔트로피를 추정하며, 이를 각각 H_r과 H_c라 하자. 엔트로피 갱신 단계에서는 $\min\{H_c, H_r\} < 0.5H_I$인 경우 실패로 판정하고, 그렇지 않은 경우 $H=\min\{H_I, H_c, H_r\}$로 잡음원의 엔트로피를 갱신한다. 이를 통해 엔트로피 갱신 단계는 재시작으로 발생할 수 있는 엔트로피 저하로부터 시간과 위치의 종속성을 검출하기 위함으로 보인다.

Ⅲ. 재시작 검정의 실험적 분석

3.1 실험 설정

재시작 검정을 통과한 잡음원은 재시작 출력 수열이 위치에 독립이고, 예측에 추가적인 이점을 제공하지 않으며, 같은 분포에서 생성됨을 보장받는다. 본 장에서는 같은 분포에서 생성됨을 보장해주는 재시작 검정의 특징에 주목하여, 재시작 검정이 분포 변화 감지법으로 활용될 수 있는지 확인한다. 독립성이 깨지거나 다음 값 예측에 이점을 주는 현상을 통제하기 위해, Quantis 양자난수발생기[3]를 활용하여 실험 데이터를 생성하였다.

실험은 다음의 상황을 가정한다. 잡음원 샘플은 크기가 2 비트이며, 출력 값을 $i=0,1,2,3$으로 갖는 확률변수 Y라 할 때, 평가자는 잡음원의 출력 분포가 $P(Y=i) = \begin{cases} 0.7, & \text{if } i=0 \\ 0.1, & \text{if } i=1,2,3 \end{cases}$을 따른다고 주장한다. 평가자는 SP 800-90B 절차대로 잡음원 검증을 진행한다. 잡음원은 IID/Non-IID 분포 판정에 의해 I.I.D.로 판정되었고, IID track에서 2 비트당 0.504 비트의 엔트로피로 추정되었다. 추정된 엔트로피 H_I는 재시작 검정에서 고정된 값이며, 건전성 검사의 최대 발생 빈도 추정에 사용된다.

3.2 실험 1 - 엔트로피 저하가 발생된 분포 변화

엔트로피 소스로 활용될 수 있는 TRNG의 대부분은 물리적 현상의 예측 불가능성을 이용하여 난수를 생성한다. TRNG의 경우, 환경 변화나 장비의 노후로 인해 같은 값이 계속해서 출력되는 현상이 발생한다[4]. 실험 1은 이러한 상황에 대한 실험으로, 재시작 검정을 진행하는 중 난수발생기의 501번째 재시작 시점부터 [그림 2]와 같이 잡음원 출력의 분포가 $P(Y=i) = \begin{cases} 0.8, & \text{if } i=0 \\ (0.2)/3, & \text{if } i=1,2,3 \end{cases}$로 변화했다고 가정한다.

[그림 2] 엔트로피 저하가 발생된 분포의 변화

3.3 실험 2 - 엔트로피 저하가 발생되지 않은 분포 변화

실험 2는 엔트로피가 저하되지 않으면서 분포가 변한 경우에 재시작 검정이 분포 변화를 탐지할 수 있는지 확인하기 위해 진행한다. 잡음원 출력의 분포는 [그림 3]과 같이 501번째 재시작을 진행한 시점부터 $P(Y=i) = \begin{cases} 0.7, & \text{if } i=1 \\ 0.1, & \text{if } i=0,2,3 \end{cases}$로 변화했다고 가정한다.

[그림 3] 엔트로피 저하가 발생되지 않은 분포의 변화

3.4 실험 결과

실험 1은 건전성 검사에서 분포 변화가 탐지되었지만, 실험 2의 경우에는 분포 변화를 탐지하지 못하였다. 이 결과는 재시작 검정이 엔트로피가 저하로 인한 분포 유지에 실패를 검출하기 위해 설계되었기 때문으로 보인다. 즉, 재시작 검정은 실험 1과 같이 엔트로피가 저하되는 방향으로 분포를 유지하지 못하는 경우를 탐지할 수 있음을 보여준다.

Ⅳ. 결 론

본 논문에서는 분포 변화 탐지 관점에서 NIST의 재시작 검정을 조사 분석하였다. 실험적 분석을 통해 재시작 검정은 엔트로피가 저하되어 분포가 유지되지 못하는 경우를 탐지할 수 있음을 확인하였고, 이는 재시작 검정의 설계 사상으로 인해 가능하였으므로 분석하였다. 추후 연구로는 두 분포 사이의 변화를 탐지하는 기술을 적용한 엔트로피 추정법을 주제로 연구를 진행할 예정이다.

참 고 문 헌

[1] NIST, Recommendation for the Entropy Sources Used for Random Bit Generation, NIST Special Publication 800-90B, 2018.

[2] J.S. Kang, H. Park, and Y. Yeom, “Probabilistic Analysis for the Relationship Between Min-Entropy and Guessing Attack”, Advanced in Computer Science and Ubiquitous Computing, 2016.

[3] ID Quantique, Retrived Jul., 15 from https://www.idquantique.com/random-number-generation/overview/.

[4] A. Muthukumar, N. Sivasankari, and K. Rampriya, “Anti-Aging True Random Number Generator for Secured Database Storage”, 2017 4th International Conference on Advanced Computing and Communication Systems, IEEE, 2017.