이진 수열의 임의성 검정을 위한 통합용 패키지

신 원†, 김혜정†, 이경현†, 신종태‡
† 부경대학교 전자계산학과, ‡ 한국정보보호센터

An Integrated Package for Randomness Tests of Binary Sequences

Weon Shin†, Hea-Jeong Kim†, Kyung-Hyune Rhee†, Jong-Tae Shin‡
† Dept. of Computer Sicence, Pukyong National University
‡ Korea Information Security Agency

요 약

본 논문에서는 비밀성 메커니즘의 암호학적인 안전성에 대한 체계적인 분석을 통하여 난수열의 각종 암호학적, 통계적 성질에 기반한 평가 기법을 소개하고 이를 패키지로써 구현하였다. 본 패키지는 기존의 알려진 통계적 검정 기법들 뿐만 아니라 다양한 암호학적 특성에 기반한 검정 기법들을 종합적으로 분석하여 구현함으로써 차후 개발이 예상되는 새로운 스트림 및 블록 암호 알고리즘의 설계와 안전성 평가에 유용하게 적용될 수 있다.

1. 서론

컴퓨터 보급이 확대되고 정보 통신 기술이 급격히 발달함에 따라 통신망에서의 정보 보호에 대한 요구가 급격히 증가되고 있다. 다양한 정보 보호기술을 기반으로 암호 시스템을 구축하여 사용하고 있으며 이러한 암호 시스템의 구현을 위한 암호 알고리즘, 즉 비밀성 메커니즘에 대한 연구가 활발히 진행되어 오고 있다. 비밀성 메커니즘들에 대한 암호학적인 안전성은 키 수열의 임의성(randomness)에 크게 의존한다. 실제 사용되는 키 수열은 난수 발생기로부터 결정적 방법에 의해 생성된 의사난수열(pseudo-random sequences)이므로 엄밀한 의미에서의 완전한 난수열이라 할 수 없다. 따라서, 생성된 수열의 임의성 여부와 이를 정량적으로 평가할 검정 기법들이 필요하게 된다[11]. 비밀성 메커니즘은 크게 스트림과 블록으로 나눠 질 수 있으며 이에 대한 체계적인 분석을 통한 난수열의 안전성 및 각종 수학적, 통계적 성질[12][13]들에 대한 종합적 평가 기법은 암호 알고리즘의 안전성 평가를 위해 필수적으로 연구되어져야 하는 분야이다.

본 논문에서는 암호 알고리즘의 임의성 관점의 안전성 검증을 위해 각종 검정법들을 비교 분석하였으며, 기존의 몇몇 검정에 대한 개선 방안이 제시되고 있다. 이러한 암호학적 특성을 고려한 각종 평가 기법들의 이론 정립과 구현은 비밀성 메커니즘의 안전성 평가뿐만 아니라 안전한 암호 시스템의 설계에 유용하게 활용될 수 있을 것이다.

2. 여러 가지 임의성 검정

2.1 일반적 통계 검정

확률 및 통계의 이론으로부터 임의성에 대한 많은 검정법들이 알려져 있으나 그 중에서 암호학적 측면에서 의미있고 또한 현실적으로 사용하기에 유용한 방법들을 소개한다.

빈도 검정(Frequency Test)

n비트 대상 수열에 대해 0과 1의 수가 균일하게 분포하고 있는지를 검정한다. 대상 수열로부터 0 및 1의 개수를 구하여 다음과 같은 χ^2 통계량을 얻는다.

$$\chi_0^2 = \frac{(n_0 - n/2)^2}{n/2} + \frac{(n_1 - n/2)^2}{n/2} = \frac{(n_0 - n_1)^2}{n}$$

(여기서, n_0는 '0'의 측정치, n_1은 '1'의 측정치)

통계량의 기각역은 $\chi_0^2 > \chi^2(1,\alpha)$이다.

포커 검정(Poker Test)

n비트 대상 수열에서 임의의 m 비트의 패턴을 고려하는 검정이다. 검정의 목적은 주어진 수열의 각 m비트 패턴이 동일하게 나타나는지를 결정한다. 검정 통계량은 다음과 같다.

$$\chi_0^2 = \frac{2^m}{k}\left(\sum_{i=1}^{2^m} n_i^2\right) - k$$

(여기서, m은 양의 정수이며 $k = \lfloor \frac{n}{m} \rfloor$)

통계량의 기각역은 $\chi_0^2 > \chi^2(2^m - 1,\alpha)$이다.

계열 검정(Serial Test)

대상 수열에서 00, 01, 10, 11의 비트 쌍이 고려되어지며 한 비트가 그 다음 비트로 가는 전이확률을 검정한다. 이를 위한 통계량은 다음과 같다.

$$\chi_0^2 = \frac{4}{n-1}(n_{00}^2 + n_{01}^2 + n_{10}^2 + n_{11}^2) - \frac{2}{n}(n_0^2 + n_1^2) + 1$$

통계량의 기각역은 $\chi_0^2 > \chi^2(2,\alpha)$이다.

런 검정(Run Test)

n비트 대상 수열에 존재하는 다양한 길이의 0이나 1이 연속하는 run들의 수가 이상 난수열에서 기대되는 것처럼 고려될 수 있는지를 결정하기 위한 검정이다. 길이 n의 난수열에서 길이 i의 0의 연속(또는 1의 연속)의 기대치는 $e_i = (n-i+3)/2^{i+2}$이며, 검정 통계량은 다음과 같다.

$$\chi_0^2 = \sum_{i=1}^{L}\frac{(B_i - e_i)^2}{e_i} + \sum_{i=1}^{L}\frac{(G_i - e_i)^2}{e_i}$$

통계량의 기각역은 $\chi_0^2 > \chi^2(2(L-1),\alpha)$이다.

자기상관 검정(Autocorrelation Test)

n비트 이진 수열 $s^n = s_0, s_1, \cdots, s_{n-1}$이 주어졌을 때 s^n에서 d 비트만큼 전이시켜 생성한 수열 s^{n+d}과의 상관 관계를 조사하는 검정이다. 이때 새로 구성된 수열에 관한 도수-1 검정을 원래의 수열에 관한 delay가 d인 자기상관 검정이라고 한다.

$$\chi_0^2 = \frac{(n_0 - n/2)^2}{n/2} + \frac{(n_1 - n/2)^2}{n/2} = \frac{(n_0 - n_1)^2}{n}$$

통계량의 기각역은 $\chi_0^2 > \chi^2(1,\alpha)$이다.

2.2 스트림 암호 알고리즘 검정

본 절에서는 스트림 암호 알고리즘의 안전성을 종합적으로 평가하기 위해 다양한 관점의 검정이론을 소개하고 분석한다.

엔트로피 검정(Entropy Test)

엔트로피가 수열의 난수성에 대해 유용한 검정 근거를 제공한다[6][7]는 제안에 의해 엔트로피의 이산 형태에 기초한 일양성과 독립성을 아래의 알고리즘을 사용하여 검정[5]한다.

<검정 알고리즘>

단계 1 : 길이 L인 n개의 비트 스트링을 잡고, 확률 변수 Y_i를 i 번째 위치($i = 1, \cdots, n$)에서부터 시작하는 길이 L의 비트 스트링에 의해 표현되는 정수라 둔다.

단계 2 : Y_i에 의해 j의 number인 $X_j = \sum_{i=1}^{n} I[Y_i = j]$와 sample 엔트로피인 $H = -\sum_{j=0}^{k-1}(X_j/n)\log_2(X_j/n)$를 정의하고 구해진 H를 H_1로 둔다.

단계 3 : $n+1$비트를 가지고 동일한 절차를 $2n$까지 반복하고, 엔트로피 값 H_2를 산출하는 방식으로 계속한다.

단계 4 : $i \geq 1$에 대해, H_i는 비트 $(i-1)n+1, \cdots, in$를 순환적으로 두고 그 순환상에서 연속되는 비트 L의 모든 n 스트링들을 관찰함으로써 구해지는 H 값이 된다.

단계 5 : 표준화 값들인 $Z_1, \cdots, Z_N$을 계산한다. 큰 수 N에 대해, $\sqrt{N}\,Z_N = \frac{1}{\sqrt{N}}\sum_{i=1}^{N} Z_i$이고 이는 H_0상에서 근사적으로 $N(0,1)$이 된다.

Maurer의 Universal 검정

난수 생성기에 대한 Maurer의 Universal 검정[1]은 기존의 통계적 관점의 검정에 비해 좀더 일반적인 통계적 모델을 기반으로 한다. 검정 통계치 T는 양의 정수 값인 파라미터 L, Q, K에 의해 설정된다. 검정을 수행하기 위해, 전체 길이 N인 이진 수열 $s^N = s_0, s_1, \cdots, s_{N-1}$에서 겹치지 않는 인접한 길이 L의 블록을 만든다. 수열 s^N의 전체 길이는 $N = (Q+K)L$이다. 여기서, K는 검정 단계의 블록 개수이고 Q는 초기화를 위한 블록 개수이다. $A_n(s^N)$을 n번째 블록과 처음으로 일치하게 되는 $n-i$번째 블록이 존재할 경우 i로 정의하고 그렇지

않을 경우 n로 정의한다. 정규분포를 따르는 다음의 통계량을 이용하여 검정을 수행한다.

$$Ts^N = \frac{1}{K}\sum_{n=Q}^{Q+K-1} \log_2 A_n(s^N)$$

선형 복잡도 검정(linear complexity test)

수열 $s^n = s_0, s_1, \cdots, s_{n-1}$의 선형 복잡도를 결정하기 위한 검정법이며 선형 복잡도란 s^n을 생성하는 가장 짧은 LFSR(Linear Feedback Shift Register)의 길이를 의미한다. 다음의 검정 알고리즘은 수열 s^n의 선형 복잡도 $L(s^n)$을 출력한다.

<검정 알고리즘>

단계 1 : 초기화.

$C(D) \leftarrow 1,\ L \leftarrow 0,\ m \leftarrow -1,\ B(D) \leftarrow 1,\ N \leftarrow 0$

단계 2 : $N < n$인 동안 다음의 과정을 반복한다.

2.1 next discrepancy d를 계산한다.

2.2 만일 $d = 1$이면 다음을 수행한다.

$T(D) \leftarrow C(D),\ C(D) = C(D) + B(D)D^{N-m}$

만일 $L \le N/2$이면

$L \leftarrow N+1-L,\ m \leftarrow N,\ B(D) \leftarrow T(D)$

2.3 $N \leftarrow N+1$

단계 3 : L값을 출력한다.

선형 복잡도 프로파일 검정
(Linear Complexity Profile Test)

LCP(Linear Complexity Profile)는 스트림 암호 시스템의 비도를 결정하는데 가장 중요한 역할을 하는 요소 중의 하나이다. n비트 수열 $s^n = s_0, s_1, \ldots, s_{n-1}$에 대한 수열 $L_1, L_2, \ldots, L_n$을 이용하여 $n \times L$ 평면을 구성하였다. 각 (n, L_n) 정점에 의한 그래프를 출력함으로써 전체 수열의 비트 수 증가에 따른 LC의 분포 성향을 분석할 수 있도록 하였다.

Zip-Lempel 복잡도 검정
(Zip-Lempel Complexity Test)

ZLC(Zip-Lempel Complexity) 검정은 수열의 반복성의 정도를 나타내는 측도이며 수열에서 어떤 한 개의 부분 수열도 이전에는 일어나지 않도록 분해되어진 부분 수열의 개수, 즉 수열을 따라 움직일 때 나타나는 새로운 패턴의 개수를 말한다. 이러한 특성을 이용하면 주어진 이진 수열의 동일한 패턴의 반복정도를 알 수 있고 평균 패턴 길이와 ZLC를 구할 수 있으며 어느 이진 수열의 각 패턴 길이와 ZLC를 구하여 이와 비교한 후, 평균값에 크게 미치지 못하는 수열은 랜덤하지 않은 수열로 판정할 수 있다.

Walsh-Power Spectrum 검정

Walsh-Power Spectrum 검정은 자기 상관함수가 δ-함수가 된다는 사실을 이용하여 주어진 수열의 비상관성(uncorrelatedness)을 검정하는 통계적 검정법이다[9]. Power Spectrum 검정은 자기상관 함수에 감춰져 있을지 모르는 어떤 주기성을 찾아서 관측 가능하도록 확대하는 것과 같은 효과를 지닌다. Walsh Band Spectrum을 이용한 임의성 검정법에서는 주어진 수열 $\{u_n\}_{n=0}^{2^n-1}$의 Walsh-Power Spectrum을 이용하여 비상관성을 검정한다. 2^{n-m}이 충분히 클 때 이항분포를 정규분포로 근사하여 $N(\alpha)$가 위와 같은 유의수준의 신뢰구간에 속하면 주어진 수열은 Walsh-Power Spectrum 검정을 통과하게 된다.

New Universal 검정

New Universal 검정[1]은 다음 비트 검정(next bit test) 이론을 바탕으로 하였으며 이는 난수 생성기에 의해 생성되어진 수열의 임의의 i 비트들에 대해 1/2 이상의 성공 확률을 가지고 i 비트들의 다음 비트를 예측하려는 것이다. 다음 비트 검정이 일반적인 검정으로서의 성질을 가진다는 것이 Yao[3]에 의해 증명되었다. 아래의 알고리즘에 의한 검정 결과를 이용하여 다음에 예측되어지는 비트들의 수에 대한 노드들의 수가 주어지는 히스토그램을 구성하여 수열의 지역적 비난수 성향뿐만 아니라 전역적 비난수 성향을 분석해 볼 수 있다.

<검정 알고리즘>

단계 1 : 결정 임계치 α값을 다음과 같이 계산한다.

$$\alpha = \frac{1+\sqrt{\chi^2/n}}{2}$$

단계 2 : $l = round(\log_2(n))$을 계산한다.

단계 3 : 스트링의 꼬리에 스트링의 처음 부분에 나타나는 l-1개의 비트들을 덧붙이고 스트링을 서로 겹쳐 가면서 l 비트의 단위로 나눈다.

단계 4 : 각각의 블록을 비교해 나가면서 길이 l을 갖는 각 패턴의 발생 횟수를 계산한다.

단계 5 : 계층 l과 l-1에서 트리를 형성해 나가면서 각 간선에 대응되는 확률을 구한다.

단계 6 : 계층 l-1에 있는 각 노드에 대해 만일 다음 비트가 α보다 더 높은 확률을 가지고 나타난다면 다음 비트는 예측되어질 수 있으며 그렇지 않은 경우 다음 비트는 결정될 수 없다.

단계 7 : 계층 l-1에 있는 각 노드에 대해 이후에

예측되어질 수 있는 스트링의 길이를 계산한다.

2.3 블록 암호 알고리즘 검정

블록 암호는 고정된 크기의 입력 블록을 고정된 크기의 출력 블록으로 변환하는 알고리즘이다. 본 논문에서는 여러 가지 블록 암호의 안전성 평가 기술들 중에서 정량화가 가능한 암호 로직, 대수적 구조, 통계적 관점의 검정을 수행하며 동작 모드에 따라 일반 통계 검정 및 스트림 암호 알고리즘 검정법이 적용 가능하다.

쇄도 효과 검정(Avalanche Effect test)

블록 암호에서 평문과 키 비트는 출력 전체의 비트에 고루 영향을 끼쳐야 한다. 이러한 출력 비트들의 변화량은 입력 1비트를 변화시켰을 때 생기는 출력과 원래 출력들간의 Hamming 거리로서 조사하며 이때 나타나는 출력의 변화를 쇄도 효과라 하고 다음과 같이 정의한다.

$$\sum_{x\in Z_2^n} wt(f(x)\oplus f(x\oplus c_i^{(n)})) = m2^{n-1}$$

(여기서, $wt(\cdot)$는 Hamming 가중치 함수이고, $1\le i\le n$)

쇄도 효과에서는 입력 비트가 1bit가 변했을 때 평균적으로 출력 비트의 절반이 변해야 한다.

입출력 의존성 검정
(Input-Output Dependence test)

엔트로피를 이용한 입출력 의존성 검정은 Substitution-Permutation 네트워크 암호 시스템에 있어서 S-box의 입출력 사이의 의존도를 검정한다. 정보 이론에 근거한 두 개의 확률 변수 X, Y의 상호 정보량 $I(X;Y)=H(X)-H(X|Y)$를 이용한다. 단, $H(X)$는 확률변수 X의 엔트로피(불확실성)로써, $H(x)=-\sum_i P(x=i)\log P(x=i)$로 나타낸다. X를 입력에 대한 벡터, Y를 출력에 대한 벡터로 간주하여 상호 정보량을 입출력에 대한 정보누수 측도(*IOILM*, Information Leakage Measure)는 입력이 출력으로 그대로 빠지는 누수현상에 대한 정량화된 측도로 사용할 수 있다. 입력 x_i와 출력 y_i를 갖는 $m\times n$ S-box에 대해, 처음 출력 비트에 대한 *IOILM*1은 다음과 같으며 알려져 있지 않은 값들은 항상 최대 가능 엔트로피를 갖는다고 가정한다.

$$IOILM1 = \frac{1}{m}\left(m - \sum_{i=1}^{m} H(y_1 \mid x_i)\right)$$

또한 order r에 대한 Input-Output Dependence Criterion은 r 입력 값들을 알고있는 것이 출력 값들에서의 불확실성을 줄이지 못하게 하는 S-box들을 선택하는데 사용된다. S-box가 order r의 Input-Output Dependence criterion를 만족한다는 것은 다음의 식과 동치가 된다(여기서, $r<m$).

$$Prob(y_i \mid a_1x_1,\cdots,a_mx_m) = Prob(y_i)$$

비선형성 검정(Nonlinearity Test)

비선형성은 여러 가지로 정의할 수 있지만, 여기서는 affine 함수와의 최대 거리로 비선형성을 정의한다. 부울함수 F가 특수한 성질을 만족할 때 F의 비선형성에 대해 살펴보면, F가 선형이면 $N_F=0$이고, F가 벤트(bent) 함수이면 $N_F=2^{n-1}-2^{n/2-1}$이다. 벤트함수는 비선형성이 가장 좋은 것이나 균형이 아니고 벤트 함수가 존재할 필요조건은 $n\ge 2m$, n은 짝수이다. 따라서 암호 논리로 사용되는 부울함수는 비선형성이 좋은 Almost Bent이며, 이 경우 $N_F=2^{n-1}-2^{n/2-1/2}$이다. 이상의 결과에 의해 부울함수의 비선형성은 다음과 같이 검정한다.

(1) $N_F\ge 2^{n-1}-2^{\lfloor n/2\rfloor}$이면 비선형성이 좋다("Good"으로 표시).

(2) $N_F=0$이면, 비선형성은 나쁘다("Bad"로 표시).

(3) $0<N_F<2^{n-1}-2^{\lfloor n/2\rfloor}$이면 비선형성이 보통이다("Ordinary"로 표시).

균형성 검정(Balanced Test)

함수 $f:\{0,1\}^n\to\{0,1\}$가 부울함수일 때 0과 1의 값을 가질 가능성이 같은, 즉

$$\#\{x\mid f(x)=0\} = \#\{x\mid f(x)=1\}$$

인 함수를 균형(balance)라고 정의한다. 벡터값을 갖는 부울함수의 균형성 정의도 같은 방법으로 정의한다. 즉, $F:\{0,1\}^n\to\{0,1\}^m$ $(n\ge m)$가 벡터값을 갖는 부울함수일 때 $\{0,1\}^m$상의 값을 가질 가능성이 같은, 즉 임의의 벡터 $b\in\{0,1\}^m$에 대해 $\#:\{x\mid F(x)=b\}=2^{n-m}$인 함수를 균형이라고 정의한다. 균형성 검정을 수행할 때, S-Box가 균형이면, "Balanced", 균형이 아니면 "No Balanced"가 출력된다.

이진 유도 검정(Binary Derivative Test)

이진 수열의 블록 패턴의 비율이 같은지를 검정하는 방법이다. 검정 알고리즘은 다음과 같으며 수열이 임의성을 갖는다면 binary derivative 수열에서 '0'과 '1'의 비율이 거의 같아야 한다.

<검정 알고리즘>

단계 1 : 수열 $s^n=s_0,s_1,\cdots,s_{n-1}$으로부터 연속적인 2비트를 exclusive-or함으로써 길이 $n-1$인 이진 수

열을 생성하여 1차 binary derivative를 구한다.
단계 2 : 1차 binary derivative로부터 2차 binary derivative를 구한다.
단계 3 : 위의 단계를 반복하여 i차 binary derivative 수열에서 '0'과 '1'의 비율을 조사한다.

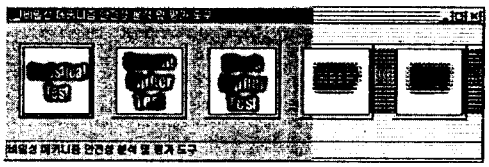
논리적 폐쇄 검정(Switching Closure Test)

논리적 폐쇄 검정은 수열의 대수적 안전성을 검정한다. 임의의 평문, 암호문 쌍 (p,c)에 대해서 $E(x,p)=D(y,c)$를 만족하는 쌍 (x,y)를 고려하는 검정이다. 만일 조건을 만족하는 쌍 (x,y)를 발견하면 암호시스템은 검정을 통과하지 못하는 것이고 그렇지 않고 수 차례의 시도에도 (x,y)를 찾지 못하면 암호시스템은 검정을 통과하는 것이다.

3. 시뮬레이션 및 결과 분석

3.1 시뮬레이션 환경

비밀성 난수 검정 패키지는 Pentium(100MHz) PC의 Windows 98 환경을 갖춘 시스템에서 윈도우즈용 프로그램 개발도구인 Borland Delphi 4.0으로 구현하였다. 본 패키지는 GUI 방식의 사용자 인터페이스를 도입하여 각 검정에 따른 매개변수 값을 설정하여 원하는 결과를 얻을 수 있게 하였다. 비밀성 난수 검정 패키지는 스트림 암호용 검정 프로그램과 블록 암호용 검정 프로그램, 그리고 스트림과 블록에 공통적으로 적용이 가능한 통계적 검정 프로그램으로 구성된다.



<그림1> 구현된 비밀성 메커니즘 분석 및 평가 패키지

3.2 스트림 암호 알고리즘 검정

스트림 암호 알고리즘으로 RC4(Ron's Code 4), SEAL(Software-optimized Encryption ALgorithm), HASP(Hybrid Algorithm of Stream and Permutable s-box)이 적용되었으며 검정 패키지에 적용된 소스 크기는 동일하게 1Mbit로 하였다. 일반적 통계 검정과 스트림 암호 알고리즘의 검정 기법으로 위의 각 알고리즘에 의해 생성된 난수열에 적용하였으며, 몇몇 기법을 제외하고 대부분 검정을 통과하였다. 특히 New Universal 검정은 난수열의 전역적인 비난수 성향과 지역적인 비난수 성향을 히스토그램을 사용하여 출력해 줌으로써 결과 분석이 용이하게 이뤄지도록 하였다. 검정 결과는 다음과 같다.

검 정	적용 알고리즘		
	RC4	SEAL	HASP
Entorpy	통과×	통과○	통과○
누적 z_a 값	1.05E-05	0.00848	0.01922
임계값	별도의 표 참조		
Maurer's Universal	통과×	통과×	통과×
z_a 값	16.68801	16.68746	16.6900
임계값(5%)	-1.96 ~ 1.96		
Walsh-Power Spectrum	통과○	통과○	통과○
$M(a)$	50	53	39
임계값(5%)	35.5 ~ 62.2		

<표1> 스트림 검정 결과

3.3 블록 암호 알고리즘 검정

블록 암호용 검정 프로그램에 적용된 블록 암호 알고리즘은 일반적으로 잘 알려진 DES의 S-box가 사용되었다. 암호 로직의 검정을 위해서는 균형성, 비선형성, 쇄도 효과, 입출력 의존성 검정이 사용되었고 대수적 안전성 검정을 위해서는 논리적 폐쇄 검정법이 적용되었다. 그 외에 블록 암호의 임의성을 측정하기 위해서는 이진 유도 검정이나 통계적 검정법들을 이용하면 된다.

① 쇄도 효과 검정

검정에 적용된 암호 알고리즘은 DES와 BADI(Block Algorithm with Double Involution)가 사용되었으며, BADI는 49%의 쇄도 효과(Avalanche Effect)를 보였다.

② 균형성 검정

균형성 검정은 S-box의 크기를 최대 입력 32, 출력 16으로 설정할 수 있으며, 본 시뮬레이션에서는 입력 값으로 6, 출력 값으로 4를 설정하여 시행하였으며, 검정 결과는 "No Balanced"를 출력한다.

③ 이진 유도 검정

주어진 수열에 대해서 Binary Derivative를 최대 20차까지 출력해 볼 수 있으며 각각에 대한 '0'과 '1'의 비율을 출력한다.

④ 논리적 대수 검정

사용자가 지정한 임의의 평문과 암호문에 대해 서로 연관성을 가지는지를 검정한다.

⑤ 입출력 의존성 검정

입력 비트가 8이고 출력 비트가 8인 S-box에 대해

입력 비트에 대한 모든 경우의 수에 대한 출력 값을 나타내고 출력 1 비트의 위치를 고정시켰을 때 입력 비트와 동일한 값을 가질 확률을 리스트화 해서 나타내도록 하였다. 이때 고정시킨 8개의 출력 비트에 대한 *IOILM*을 산출한다.

⑥ 비선형성 검정

비선형성 검정은 S-box의 크기를 최대 입력 8, 출력 8비트로 설정할 수 있으며, 본 시뮬레이션에서는 입력을 6비트 출력을 4비트로 하여 시행하였다. 평균 비선형성 값은 24이며, 비선형성이 "Ordinary"인 검정 결과를 가진다.

3.4 통계적 검정

통계적 검정은 스트림 암호 검정과 블록 암호 검정에 공통적으로 적용할 수 있으며, 본 논문에서는 스트림 암호 검정에 사용된 데이터에 대해서 통계적 검정을 수행하였다. 검정 결과는 다음과 같다.

검 정	적용 알고리즘		
	RC4	SEAL	HASP
빈도 검정	통과○	통과○	통과○
χ^2 값	1.19246	0.00102	0.66912
임계값(5%)	$\chi^2(1,\alpha)=3.84146$		
포커 검정	통과○	통과○	통과○
χ^2 값	229.72569	281.13050	255.09222
임계값(5%)	$\chi^2(255,\alpha)=293.24777$		
계열 검정	통과○	통과○	통과○
χ^2 값	3.63356	0.02682	2.39508
임계값(5%)	$\chi^2(2,\alpha)=5.99148$		
런 검정	통과×	통과×	통과○
χ^2 값	92.61930	54.05089	34.705596
임계값(5%)	$\chi^2(28,\alpha)=41.33715$		
자기상관 검정	통과×	통과×	통과○
χ^2 값	4.548164	3.897663	0.165889
임계값(5%)	$\chi^2(1,\alpha)=3.84146$		

<표2> 통계적 검정 결과

4. 결론

본 논문에서는 비밀성 메커니즘의 안전성 평가 도구로서 이진 수열의 임의성 검증을 위해서 여러 가지 방법들을 고찰해 보았다. 먼저, i,i,d 관점의 일반 통계적 검정을 위해 빈도의 편향성(빈도 검정, 포커 검정)을 검정하고, 각 항 사이의 독립성을 검정(계열 검정, 런 검정, 자기상관 검정)한다. 이러한 통계적 검정법들은 스트림과 블록 알고리즘에 의해 생성된 난수열에 대해 공통적으로 적용할 수 있다. 스트림 암호 알고리즘 검정법에서는 엔트로피 관점의 검정(엔트로피 검정, Maurer의 Universal 검정), 선형 복잡도 관점의 검정(LC 검정, LCP 검정, ZLC 검정), 이진 수열의 비상관성 검정(Walsh- Power Spectrum 검정), 그리고 다음 비트 검정 기법에 기반한 New Universal 검정법이 적용되었다. 블록 암호 알고리즘 검정법에서는 비선형성을 조사하기 위한 쇄도 효과 검정, 입출력 의존성 검정, 비선형성 검정, 균형성 검정, 이진 유도 검정, 논리적 폐쇄 검정법이 적용되었다. 특히 엔트로피 검정에 있어서 기존의 non-overlapping 엔트로피 검정보다 암호학적인 결점을 찾아내는데 좀더 많은 정보를 이끌어 낼 수 있는 overlapping된 엔트로피 검정을 적용하였다. 이와 같이, 본 논문에서는 안전성 관점의 비도 요인을 체계적으로 분석하여 통합 패키지로 구현함으로써 난수열의 안전성에 대한 정량적 평가 도구를 제공하고 비밀성 메커니즘의 안전한 설계를 위한 기준을 제시하고 있다.

참 고 문 헌

[1] U.M.Maurer, "A universal statistical test for random bit generators", Journal of Cryptology, Vol. 5, No. 2, pp.89-105, 1992.

[2] B.Sadeghiyan and J.Mohajeri, "A new universal test for bit strings", ACISP'96, pp.311-320, 1996.

[3] A.Yao, "Theory and application of trapdoor functions", Proc. 23rd FOCS, pp. 80-91, 1982.

[4] A.Schrift and A.Shamir, "Universal tests for nonuniform distributions", Journal of Cryptology, Vol. 6, No. 3, pp.119-113, 1993.

[5] P.L'Ecuyer, "Entropy Tests for Random Number Generators", ACM Transactions on Modeling and Computer Simulation, 1997.

[6] A.Compagner. "Operational conditions for random number genration", Physical raeview E, 52(5-B):5634-5645, 1995.

[7] P.L'Ecuyer, "Random Number Generators and Empirical Tests", vol. 127 of Lecture Notes in Statistics, 124-138, New York : Springer.

[8] J.Ziv, "Compression tests for randomness and estimating the statistical model of an individual sequences", Sequences, pp.366-373,

1990.

[9] R.A.Rueppel, "Analysis and Design of Stream Ciphers", Springer-Verlag Berlin, Heidelbelberg 1986.

[10] K.G.Beauchamp, "Applications of Walsh and Related Functions", University of Lancaster, ACADEMIC PRESS, 1984.

[11] 한국과학기술원, "Randomness 특성 분석에 관한 연구", 한국전자통신연구소, 1991.

[12] S.Brands and R.Gill, "Cryptography, Statistics and Pseudorandomness.1", Probability and Mathematical Statistics Vol.15, pp.101-114, 1995.

[13] S.Brands and R.Gill, "Cryptography, Statistics and Pseudorandomness.2", Probability and Mathematical Statistics Vol.16, Fasc.1, pp.1-17, 1996.

[14] W.Meier and O.Staffelbach, "Nonlinearity Criteria for Cryptographic Functions", Proc. of EUROCRYPTO'89, 1989.

[15] Alfred J.Menezes, Paul C,van Oorschot, Scott A. Vanstone, "Handbook of Applied Cryptography", CRC Press. Inc.,1997.