Next-bit 검정 방법 분석

A Study on the Next-bit Test

요 약

본 논문에서는 next-bit 검정의 이론적 배경을 고찰하고, 실제적인 검정법으로 구현된 검정 방법에 대하여 조사 분석한다. Next-bit 검정 이론은 Schrift와 Shamir가 제시한 다양한 검정 방법을 중심으로 소개한다. 그리고 구현된 통계적 검정 방법은 ACISP'96에서 발표된 검정법과 CISC'97에서 제안된 검정법을 비교 분석한다.

1 서 론

Next-bit 검정법은 직관적으로 이미 생성된 수열로부터 앞으로 발생될 비트의 값을 예측할 수 있는지의 여부를 측정하는 것이다. Blum과 Micali[1]는 주어진 의사 난수 발생기로부터 앞으로 생성될 몇 비트를 예측할 수 있는 가능성을 측정한 것이 의사 난수 발생기를 특징지울 수 있다는 사실을 증명하였다. 그리고 Yao[2]는 next-bit 검정법이 대칭이고 독립인 의사 난수 발생기에 대한 유니버설 검정이 될 수 있음을 이론적으로 입증하였으며, Schrift와 Shamir[3]는 바이어스(bias)를 갖고 독립인 의사 난수 발생기에 대한 검정법으로는 고전적인 next-bit 검정법이 유니버설하지 않다는 사실을 밝혔다. 또한, 이들은 유니버설 검정이 되는 몇가지 검정 방법을 제시하였는데 POP 검정, WSR 검정, behavior 검정법 등이 확장된 next-bit 검정을 대신하여 유니버설한 검정으로 사용될 수 있음을 증명하였다.

한편, next-bit 검정 이론은 확률적 다항식 시간 알고리즘(probabilistic polynomial time algorithm), 다항식적 구별 불능성(polynomial indistinguishability), negligible 함수 등의 개념을 사용한 상당히 추상적인 것이어서 실제로 검정을 어떻게 실시할 것인지에 대해서는 알려진 방법이 많지 않다. ACISP'96에서 Sadeghiyan과 Mohajeri[4]는 Schrift와 Shamir가 제안한 POP 검정법을 기반으로 한 새로운 통계적 검정법을 발표하였다. 그리고 국내에서는 CISC'97에서 김혜정과 이경현[6]이 Sadeghiyan과 Mohajeri가 제안한 방법과 비슷한 통계적 검정법을 발표하였다.

본 논문에서는 이론적으로 가장 완성된 면모를 갖고있는 Schrift와 Shamir의 next-bit 검정 이론을 소개하고 그 의미를 분석하며, 실제로 next-bit 검정 이론을 구현한 검정 방법인 ACISP'96의 검정법과 CISC'97의 검정법을 비교 분석하고자 한다.

2 필요한 정의와 기호들

s_1^n은 $\{0,1\}^n$ 안의 길이 n인 수열이라하고, 수열 s_1^n의 i번째 비트를 s_i라 놓으며, $1 \le j < k \le n$인 j와 k에 대하여 s_j^k는 j번째 비트부터 k번째 비트까지의 부분 수열을 나타낸다고 하자. 어떤 함수 $f(n)$이 임의의 다항식 $poly(n)$과 충분히 큰 모든 n에 대해서 $f(n) < 1/poly(n)$을 만족할 때, 함수 f는 negligible하다고 부른다.

정의 1. S_n이 $\{0,1\}^n$ 위의 확률 분포일 때, 수열 $\{S_n\}$을 S로 표현하고 이를 의사 난수 발생기*(pseudo-random number generator : PRNG)*라 부른다.

정의 2. 모든 n에 대하여 S_n이 일량 확률 분포*(uniform probability distribution)*를 할 때, 즉, 임의의 $\sigma \in \{0,1\}^n$에 대하여,

$$P_S(s_1^n = \sigma) = \frac{1}{2^n}$$

을 만족할 때, *PRNG* S가 일량*(uniform)*이라고 한다. 여기에서 P_S는 *PRNG* S에 의해서 유도된 확률 분포를 의미한다.

정의 3. 모든 i에 대해서 $P_S(s_i = 1) = b(1/2 \le b < 1)$를 만족할 때, *PRNG* S는 *1*쪽으로 고정된 바이어스*(bias)* b를 갖는다고 말한다.

위 정의에서 $b < 1$이라는 조건으로부터 우리는 $P_S(s_i = 0)$과 $P_S(s_i = 1)$이 항상 0이 되지 않는다는 사실을 알 수 있는데 이는 조건부 확률에 의미를 부여하기 위한 조치이다.

정의 4. *PRNG* S가 독립이고 바이어스를 갖는다*(independent biased)*라는 의미는 *PRNG*가 바이어스를 갖으면서 각 비트들은 모두 독립이라는 뜻이다. 즉, 임의의 이진 수열 $\alpha \in \{0,1\}^n$에 대하여,

$$P_S(s_1^n = \alpha) = b^k(1-b)^{n-k}$$

이다. 여기에서 $k(0 \le k \le n)$는 α 안에 있는 *1*의 개수이다.

독립이면서 어떤 바이어스를 갖는 PRNG를 B로 나타내기로 하자.

정의 5. 임의의 확률적 다항식 시간 알고리즘 $D : \{0,1\}^n \to \{0,1\}$과 임의의 다항식 Q, 충분히 큰 모든 n에 대하여

$$|P_{S_1}(D = 1) - P_{S_2}(D = 1)| \le \frac{1}{Q(n)}$$

을 만족할 때, 두 *PRNG* S_1과 S_2는 다항식적으로 구별 불능*(polynomially indistinguishable)*이라고 한다.

PRNG가 다항식적으로 구별 불능이라는 뜻은 직관적으로 두 PRNG들로부터 유도된 확률 분포의 차이가 negligible하다는 것이다.

정의 6. *PRNG S와 B가 같은 바이어스 b를 갖고 다항식적으로 구별 불능일 때, PRNG S를 완전 독립(perfect independent)이면서 바이어스 b를 갖는다고 말한다.*

3 Next-bit 검정 이론

잘 설계된 PRNG로부터 생성된 비트 수열은 이미 생성된 수열로부터 다음 비트를 예측하기 어렵다는 성질을 소유해야 한다. 통계적 검정법의 한가지인 next-bit 검정법은 이러한 예측 불능성을 측정하기 위한 검정 방법이다. 이미 생성된 수열의 길이 관점에서 다항식 시간 안에 non-negligible한 양에 의해서 주어진 바이어스 보다 큰 정확도로 이미 생성된 수열로부터 다음 비트를 예측해내는 것이 어려울 때 주어진 PRNG는 next-bit 검정을 통과한다고 말한다. 원래의 next-bit 검정은 바이어스 $b = 1/2$인 경우에 대해서 정의되어 있었다. 이를 일반화하여 $1/2 \leq b < 1$인 임의의 바이어스에 대해서 정의한 것이 다음의 정의이다.

정의 7. *임의의 $1 \leq i \leq n$, 임의의 다항식 시간 확률적 알고리즘 $\mathcal{A} : \{0,1\}^{i-1} \rightarrow \{0,1\}$, 임의의 다항식 Q, 그리고 충분히 큰 모든 n에 대해서*

$$P_S\left(\mathcal{A}(s_1^{i-1}) = s_i\right) \leq b + \frac{1}{Q(n)}$$

을 만족할 때, 바이어스 b를 갖는 PRNG S는 next-bit 검정을 통과한다고 말한다.

위 정의에서 $b = 1/2$로 고정되었을 때가 고전적인 의미의 next-bit 검정법이다. 고전적인 next-bit 검정법과 구분하기 위하여 이 정의의 검정을 확장된 next-bit 검정(extended next-bit test)으로 부르기도 한다. Schrift-Shamir[3]는 next-bit 검정법이 독립성을 검정하는 데는 유니버설(universal)하지 않다는 사실을 밝혔다([3]의 정리 1). Schrift와 Shamir는 완전 독립이 아니면서 바이어스 b를 갖는 PRNG를 만들어서 이 PRNG가 next-bit 검정을 통과함을 보이므로써 next-bit 검정이 독립성을 측정하는데 부적함을 증명하였다. 더우기 그들은 next-bit 검정의 이러한 약점을 보완한 몇가지 검정 방법들을 제시하였는데 다음에 기술할 정의들이 바로 그것이다.

정의 8. (POP 검정) *임의의 $1 \leq i \leq n$, 임의의 고정된 c, 임의의 다항식 시간 확률적 알고리즘 $\mathcal{A} : \{0,1\}^{i-1} \rightarrow \{0,1,*\}$, 그리고 임의의 다항식 Q와 충분히 큰 모든 n에 대해서, 만일 $P_S(\mathcal{A}(s_1^{i-1}) \neq *) \geq 1/n^c$일 때*

$$\left| P_S\left(\mathcal{A}(s_1^{i-1}) = s_i \mid \mathcal{A}(s_1^{i-1}) \neq *\right) - b \right| \leq \frac{1}{Q(n)}$$

을 만족하면, 바이어스 b를 갖는 PRNG S는 POP(predict or pass) 검정을 통과한다고 말한다.

정의 9. (WSR 검정) 임의의 $1 \leq i \leq n$, 임의의 상수가 아닌 다항식 시간 확률적 알고리즘 $\mathcal{A} : \{0,1\}^{i-1} \rightarrow \{0,1,*\}$, 임의의 다항식 Q와 충분히 큰 모든 n에 대해서,

$$WS(\mathcal{A}, S, i) \leq 2 + \frac{1}{Q(n)}$$

을 만족할 때, 바이어스 b를 갖는 *PRNG* S는 *WSR(weighted success rate)* 검정을 통과한다고 말한다. 여기에서

$$\begin{aligned} WS(\mathcal{A}, S, i) &= \frac{1}{b} \cdot P_S\left(\mathcal{A}(s_1^{i-1}) \mid \mathcal{A}(s_1^{i-1}) = 1\right) \\ &\quad + \frac{1}{1-b} \cdot P_S\left(\mathcal{A}(s_1^{i-1}) \mid \mathcal{A}(s_1^{i-1}) = 0\right) \end{aligned}$$

이다.

정의 10. (Behavior 검정) 임의의 $1 \leq i \leq n$, 임의의 다항식 시간 확률적 알고리즘 $\mathcal{A} : \{0,1\}^{i-1} \rightarrow \{0,1,*\}$, 그리고 임의의 다항식 Q와 충분히 큰 모든 n에 대해서,

$$\left| P_S\left(\mathcal{A}(s_1^{i-1}) = 1 \mid s_i = 1\right) - P_S\left(\mathcal{A}(s_1^{i-1}) = 1 \mid s_i = 0\right) \right| \leq \frac{1}{Q(n)}$$

을 만족할 때, 바이어스를 갖는 *PRNG* S는 *behavior* 검정을 통과한다고 말한다.

Schrift와 Shamir는 위에서 기술한 세가지 검정법이 서로 같은 의미의 통계적 검정법이며, PRNG의 완전 독립성을 평가하는데 좋은 도구가 된다는 사실을 증명하였다.

정리 1. S가 바이어스를 갖는 *PRNG*일 때, 다음 네개의 명제들은 서로 동치이다.

- S는 완전 독립*(perpect independent)*인 *PRNG*이다.
- S가 *POP* 검정을 통과한다.
- S가 *WSR* 검정을 통과한다.
- S가 *behavior* 검정을 통과한다.

4 Next-bit 검정법의 구현

앞절에서 소개한 next-bit 검정 이론은 상당히 추상적이다. 그래서 이 이론을 적용하여 실제로 검정을 실시하는 것은 그리 쉬운 작업은 아닌 것으로 생각된다. ACISP'96에서 Sadeghiyan과 Mohajeri[4]가 처음으로 next-bit 검정 이론을 구현한 새로운 검정법을 발표했으며, 국내에서는 CISC'97에서 김혜정과 이경현[6]이 시뮬레이션을 포함한 검정법을 제시하였다.

본 절에서는 ACISP'96에서 소개된 검정법을 간단히 소개하고 분석하며, CISC'97에서 제안한 검정법의 문제점을 지적하고자 한다. Sadeghiyan과 Mohajeri는 Schrift와 Shamir[3]가 제시했던 POP 검정법을 다음 정의에서와 같이 확장시킨 EPOP(extended predict or pass) 검정법을 소개하였다.

정의 11. (EPOP 검정) 임의의 $1 \le i, l \le n$, 임의의 고정된 c, 임의의 다항식 시간 확률적 알고리즘 $\mathcal{A} : \{0,1\}^{i-1} \to \{\{0,1\}^l, *\}$, 그리고 임의의 다항식 Q와 충분히 큰 모든 n에 대해서, 만일 $P_S(\mathcal{A}(s_1^{i-1}) \neq *) \ge 1/n^c$일 때

$$\left| P_S\left(\mathcal{A}(s_1^{i-1}) = s_i^{i-1+l} \mid \mathcal{A}(s_1^{i-1}) \neq *\right) - b \right| \le \frac{1}{Q(n)}$$

을 만족하면, 바이어스 b를 갖는 *PRNG* S는 *EPOP(extended predict or pass)* 검정을 통과한다고 말한다.

POP 검정에서는 $i-1$까지의 수열로부터 i번째 비트인 s_i를 예측하는 확률을 계산했었는데 EPOP 검정에서는 i번째 비트부터 시작한 l개의 비트인 s_i^{i-1+l}을 예측하는 확률을 계산한다는 점이 다르다. 즉, 예측하는 비트의 개수가 한개에서 l개로 확장되었다는 의미에서 EPOP 검정이라 부른 것이다. POP 검정과 같이 EPOP 검정도 PRNG의 완전 독립성을 측정하는 좋은 도구가 된다.

정리 2. 바이어스를 갖는 *PRNG* S가 완전 독립일 필요 충분 조건은 S가 *EPOP* 검정을 통과한다는 것이다.

4.1 ACISP'96의 검정법

Sadeghiyan과 Mohajeri가 제시한 통계적 검정법은 EPOP 검정 이론을 기반으로 한다. 이들이 ACISP'96에서 소개한 통계적 검정법을 기술한다.

정의 12. s_1^n이 길이 n인 수열일 때,

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

을 결정 문턱치*(decision threshold)*라고 한다. 여기에서 χ^2은 유의 수준에 따라서 결정되는 카이 제곱 분포의 값이다.

결정 문턱치 α는 어떻게 정의되었는지는 빈도 검정(frequency test)을 살펴보면 쉽게 알 수 있다. 즉, 길이 n인 수열에서 1의 개수를 n_1, 0의 개수를 n_0라 할 때, 빈도 검정에 카이 제곱 검정을 적용할 때 사용하는 통계량은 $(n_1 - n_0)^2/n$이다. 이 통계량은 n을 크게하면 카이 제곱 분포에 수렴하므로 $\chi^2 = (n_1 - n_0)^2/n$으로 놓으면

$$\frac{n_1}{n} = \frac{1 \pm \sqrt{\frac{\chi^2}{n}}}{2}$$

이 된다. 그러므로 이경우 결정 문턱치 α가 의미하는 바는 수열 안에 들어 있는 0과 1의 비율 중에서 1/2보다 큰 값을 의미한다.

임의의 PRNG에서 생성된 길이 n인 수열을 가지고 통계적 검정을 실시하는 과정은 다음과 같다. 편의상 PRNG를 S라 하고 S로부터 생성된 검정 대상 수열을 s_1^n이라 하자.

1. 식 (1)에 의해서 결정 문턱치 α를 계산한다.

2. $l = \log_2 n$을 계산한다.

3. s_1^n의 처음 $l-1$ 비트를 s_1^n의 끝부분에 덧붙이고, 이로부터 서로 겹치는 l 비트 길이의 블록 n개를 얻는다.

4. 각 l 비트 블록들의 발생 빈도를 셈한다.

5. $l-1$층에서 l층으로 전이되는 트리를 그리고 각 간선에 대응되는 확률을 기록한다.

6. $l-1$층의 각 node에 대해서 다음 비트가 α보다 더 큰 확률로 나타나면 다음 비트는 예측된 것이다.

7. $l-1$층의 각 node에 대해서 그 이후에 예측할 수 있는 수열의 길이를 계산한다.

위와 같은 과정을 통해서 얻은 데이터를 가지고 어떻게 랜덤성을 판별하는지에 관해서 설명하자. 만일 $l-1$층의 어떤 node에서 $l+1$ 비트 이상을 예측할 수 있다면, 이것은 다음 블록을 예측할 수 있는 길이 l인 블록이 존재함을 의미한다. 그러므로 이 때에는 국소적 비랜덤성(local non-randomness)이 존재하는 것으로 판단하여 주어진 PRNG가 검정을 통과하지 못하는 것으로 결정한다. 그리고 전체적 관점에서 보면 어떤 node 이후에 예측되는 비트들의 개수에 관한 node들의 수가 주어지면 히스토그램을 그릴 수 있는데 이 히스토그램에 의해서 전체적 비랜덤성(overall non-randomness)을 탐지해낼 수 있다. 즉, 랜덤 수열의 히스토그램으로부터 벗어난 정도를 측정하여 수열의 랜덤성을 측정하는 것이다. 랜덤 수열의 히스토그램이 어떻게 구성되지는가를 다음 소절에서 설명한다.

4.2 랜덤 수열의 히스토그램

랜덤 수열의 경우 $l-1$층에서 l층으로 전이될 때 확률은 0과 1 사이의 확률 변수이다. 이 확률 변수의 값이 구간 $(\alpha-1, \alpha)$의 밖에 존재하면 다음 비트는 예측된 것이고, 안에 있으면 예측 불가인 것이다. 각각의 node에 대하여 다음 비트가 예측될 때, 관계있는 node들 사이에 선분을 그린다. 예를 들어서 node 10110으로부터 다음 비트가 1로 예측되었다면 관계있는 node는 01101이 된다. 이러한 상태의 node를 stage-1 node라 한다. 다시 node 01101의 다음 비트가 0으로 예측되었다면 관계있는 node는 11010인데 이러한 상태의 node를 stage-2 node라 한다. 이와 같은 방법으로 각기 다른 stage에 있는 node들의 개수를 셈할 수 있다. De Bruijn 수열과 같은 복잡한 수열은 stage-0 node의 개수는 $T_0 = 2^{l-1}$이다. 어떤 것으로부터도 예측되지 않는 블록이 stage-0 node이고, $l-1$층의 모든 node의 수는 2^{l-1}개이며, 검정 대상 수열 s_1^n이 De Bruijn 수열인 경우 l 비트 길이의 블록이 모두 한번씩 나타나게 되므로 $l-1$층의 각 블록이 모두 stage-0인 node를 형성한다.

$l-1$층에서 l층으로 전이되는 확률을 나타내는 확률 변수가 구간 (0,1)에서 일랑 분포(uniform distribution)를 이룬다고 가정하자. 이 때, 구간 $(1-\alpha, \alpha)$의 길이를 $\beta = 2\alpha - 1$로 놓으면, 다음

비트를 예측할 수 없는 node들의 개수는 $N_0 = \beta T_0$가 된다. 그리고 남은 $(1-\beta)T_0$개의 node들 중에서 stage-1 node의 개수는

$$T_1 = (1-\frac{\gamma}{2})(1-\beta)T_0 = \{(1-\gamma)+\frac{\gamma}{2}\}(1-\beta)T_0$$

가 된다. 여기에서 γ는 서로 다른 두 node가 같은 next stage를 갖을 확률이다. 예를 들어서 01110과 11110 다음 비트가 0으로 예측된다면 두 node의 다음 stage는 11100으로 같게 된다.

Stage-1 node들 중에서 많은 수가 다음 비트를 예측할 수 없을 것인데 이렇게 다음 stage를 예측할 수 없는 stage-1 node들의 개수는 $N_1 = \beta T_1$이고, stage-0인 node 중에서 이러한 stage-1에 이르는 것들의 개수는 $TA_1 = N_1/(1-\gamma/2)$이다. 즉, TA_1은 $l-1$층의 node 중에서 그 이후 한 비트만을 예측할 수 있는 node들의 개수를 의미한다. 비슷하게 stage-2 node의 개수는 $T_2 = (1-\beta)(1-\gamma/2)T_1$이고, stage-2 node 중에서 더이상 진전되지 않는 node들의 수는 $N_2 = \beta T_2$이며, stage-0 node 중에서 이와 같은 stage-2 node에 이르는 것들의 개수는 $TA_2 = N_2/(1-\gamma/2)^2$이다. 이 과정을 일반화 하면 다음과 같은 수식으로 정리할 수 있다.

$$\begin{aligned} T_i &= (1-\beta)(1-\frac{\gamma}{2})T_{i-1}\,, \\ N_i &= \beta T_i\,, \\ TA_i &= \frac{N_i}{(1-\gamma/2)^i}\,. \end{aligned}$$

이제 이미 계산된 α로부터 γ를 계산할 수 있다. γ는 서로 다른 두 node가 같은 다음 stage node를 갖을 확률이므로 $l-1$층의 모든 node가 같은 확률로 나타난다고 하고, 또 모든 stage에서 충돌의 확률이 일정하다고 가정하면, $\gamma = 1+2\alpha^2-2\alpha$가 된다.

위와 같은 과정을 거치면 검정 과정에서 나타나는 모든 변수의 값들을 계산할 수 있다. 먼저 결정 문턱치 α를 계산하고, 이 α로부터 β와 γ를 계산하면 $T_0 = 2^{l-1}$으로부터 축차적으로 $N_i(0 \le i \le l+1)$들의 값을 얻을 수 있는 것이다. 이로부터 우리는 그림 1과 같은 히스토그램을 얻을 수 있다.

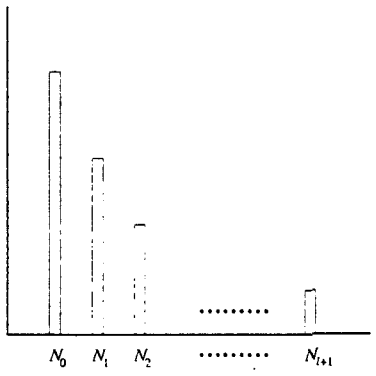

그림 1: 검정 기준 히스토그램

그림 1의 히스토그램을 토대로 검정 대상인 PRNG에 대한 랜덤성은 다음과 같은 기준에 따라서 판별한다. 랜덤한 수열이라면 실제로 측정된 stage-0 node의 개수인 T_0로부터 시작해서 얻은 N_0의 값은 히스토그램이 나타내는 값보다 크거나 같을 것이고, 반면에 $1 \leq i \leq l+1$인 i에 대해서는 측정된 N_i의 값이 히스토그램의 값보다 작을 것이다. 그러므로 검정 대상 수열 s_1^n으로부터 관찰된 통계량을 $\tilde{N}_i$라 했을 때, 각각이

$$\tilde{N}_0 \geq N_0 .$$
$$\tilde{N}_i \leq N_i \quad \forall\, 1 \leq i \leq l+1$$

을 만족하면 검정을 통과하는 것으로 판단하고, 그렇지 않으면 기각한다.

4.3 CISC'97의 검정 방법

CISC'97에서 김혜정과 이경현에 의해서 제안된 통계적 검정 방법은 ACISP'96에서 제안된 검정법을 참고하여 만들어진 것으로 보인다. ACISP'96에서는 검정 대상 수열의 길이가 약 2^l일 때, $l-1$층부터 계산해서 예측 가능한 다음 비트의 길이를 $l+1$까지 조사하여 국소적 랜덤성을 판별하였고, 전체적 관점의 랜덤성은 앞 소절의 히스토그램에 따라서 판별하였다.

한편, CISC'97에서 제안된 검정법은 검정 대상 수열의 길이가 약 2^l일 때, 1층부터 l층까지 예측 가능한 다음 비트들을 계산한 후 이를 토대로 하여 PRNG들의 랜덤성을 평가하였다. 그러나 이 방법으로 검정을 실시할 경우 국소적 랜덤성을 어떻게 탐지하는지와 전체적 관점의 랜덤성은 어떻게 평가하는지에 관한 명확한 기준이 제시되어 있지 않다. 단지 시뮬레이션 결과로부터 몇가지 PRNG들에 대한 데이터를 상호 비교함으로써 각 PRNG들에 대한 랜덤성을 평가하였다. 이렇게 랜덤성을 평가하는 것은 명확한 기준을 설정한 후에 대상 PRNG에 대하여 검정을 수행해야 한다는 통계적 검정의 기본 취지와는 거리가 있는 것으로 판단된다. 결과적으로 CISC'97에서 발표된 검정법은 몇가지 PRNG들에 대한 특성을 상호 비교해 봄으로써 PRNG들의 성능을 평가해본다는 측면에서는 의미가 있지만 일반적인 통계적 검정법으로 적용하기에는 이론적 근거가 약한 것으로 평가된다.

5 결 론

우리는 본 논문에서 next-bit 검정 이론을 고찰하고 분석하였으며, 구현된 검정법인 ACISP'96의 검정법과 CISC'97의 검정법을 비교 분석해 보았다. Next-bit 검정 이론은 이론적으로는 상당히 완성된 면모를 갖추고 있으나 그 구현이 쉽지 않다는 장애 요인을 안고 있다. 그럼에도 불구하고 ACISP'96의 검정법은 next-bit 검정의 이론적 내용을 내포한 의미있는 검정법으로 생각된다. 특히, 각 비트들 간의 독립성과 국소적 랜덤성(local randomness)을 탐지해낼 수 있는 부분은 기존 통계적 검정법에서는 쉽게 얻어낼 수 없는 측면이다. 그러나 전체적 랜덤성(overall randomness)을 평가하기 위해서 계산된 여러가지 통계량은 그 가정이 타당한지의 여부와 계산된 값에 대한 정확성 등에 있어서 개선되어야 할 부분이 있는 것으로 생각된다. 한편, CISC'97의 검정법은 몇가지

PRNG들에 대한 비교 자료를 얻는 데는 의미있는 방법이지만 일반적인 통계적 검정법으로 사용하기에는 이론적 기반이 약한 것으로 평가된다.

Next-bit 검정은 이론적으로 완성된 것이므로 이 개념을 잘 반영하여 실제적인 검정법을 구현할 수 있다면 좋은 검정 도구가 될 것이다. ACISP'96의 검정법은 향후 다양한 시뮬레이션을 통하여 그 유용성을 검증해보아야 하며, next-bit 검정 이론을 제대로 반영한 새로운 검정 도구의 개발이라는 측면에서의 연구가 필요하다고 생각한다.

참고문헌

[1] M. Blum, S. Micali : "How to generate cryptographically strong sequences of pseudo-random bits", *SIAM J. Comput.*, Vol 13, No. 4, 1984, pp. 850-864.

[2] A. C. Yao : "Theory and applications of trapdoor functions", *Proc. 23rd FOCS*, 1982, pp. 80-91.

[3] A. Schrift, A. Shamir : "Universal tests for nonuniform distributions", *J. Cryptology*, Vol. 6, No. 3, 1993, pp. 119-133.

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

[5] D. Knuth, "The Art of Computer Programing", Vol. 2, Addison-Wesley, 1973.

[6] 김혜정, 이경현 : "난수열에 대한 새로운 통계적 검정", *CISC'97 논문집*, Vol. 7, No.1, 1997, pp. 332-341.