

(19) 대한민국특허청(KR)  
(12) 등록특허공보(B1)

(51) Int. Cl.<sup>6</sup>  
G06F 11/22

(45) 공고일자 1999년06월 15일

(11) 등록번호 10-0194792

(24) 등록일자 1999년02월 10일

|           |                 |           |               |
|-----------|-----------------|-----------|---------------|
| (21) 출원번호 | 10-1995-0055851 | (65) 공개번호 | 특1997-0049244 |
| (22) 출원일자 | 1995년 12월 23일   | (43) 공개일자 | 1997년 07월 29일 |

(73) 특허권자 한국전자통신연구원 정선종  
대전광역시 유성구 가정동 161번지

(72) 발명자 박상영  
대전광역시 서구 갈마동 동산아파트 10동 702호  
김영수  
대전광역시 유성구 어은동 한빛아파트 105동 1803호  
이흥섭  
대전광역시 유성구 어은동 한빛아파트 131동 405호

(74) 대리인 박해천

심사관 : 민해정

(54) 병렬 의사 랜덤 수열 발생기에 대한 실시간 동작확인장치

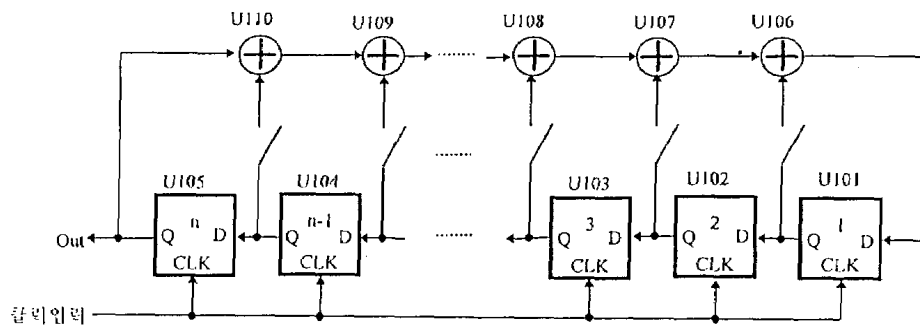
요약

본 발명은 의사 랜덤 수열 발생기를 병렬로 사용하여 랜덤한 수열을 얻는 시스템에서 각 의사 랜덤 수열 발생기의 동작 상태를 실시간으로 확인하는 장치를 제공하는데 그 목적이 있다.

이를 위해 본 발명은, 여러개의 의사 랜덤 수열 발생기 출력 중 하나를 선택하는 입력 선택 수단(1), 검사용 수열을 발생하는 검사용 수열 발생 수단(2), 상기 입력 선택 수단(1)에 의해 선택된 의사 랜덤 수열 발생기의 출력과 검사용 출력 발생 수단(2)에서 생성된 출력을 비교하여 결과를 출력하는 검사 회로 수단(3)을 구비한다.

이에 따라 본 발명은, 동일한 의사 랜덤 수열 발생기를 사용하여 출력된 수열을 사용하는 시스템의 동작 상태를 실시간으로 확인할 수 있으므로 시스템의 신뢰도를 높일 수 있다.

대표도



명세서

[발명의 명칭]

병렬 의사 랜덤 수열 발생기에 대한 실시간 동작 확인장치

[도면의 간단한 설명]

제1도는 의사 랜덤 수열 발생기로 선형 궤환 쉬프트 레지스터의 구성도.

제2도는 의사 랜덤 수열 발생기를 병렬로 사용하는 병렬 스크램블러의 예시도.

제3도는 검사용 의사 랜덤 수열 발생기의 상세 회로도.

제4도는 본 발명에 따른 병렬 의사 랜덤 수열 발생기에 대한 동작 확인 장치의 구성도.

제5도는 본 발명에 따른 병렬 의사 랜덤 수열 발생기에 대한 동작 확인 장치의 상세 회로도.

\* 도면의 주요부분에 대한 부호의 설명

1 : 입력 선택부

## 2 : 검사용 수열 발생부

### 3 : 검사 회로부

U101~U105, U311~U314 : D플립플롭

U331~U334 : AND게이트

U106~U110, U204~U206, U321~U323 :EX-OR 게이트

U301~U303 :2x1 MUX

U341 : n비트 래치

U342 : 모듈로-2합산기

## U207 : k비트 직병렬 변환기

## U208 : k비트 병렬기 변환기

U201~U203 : 의사 랜덤 수열 발생기

U501 : kx1 MUX

U502 : 이진 계수기

U503 : 검사용 의사 랜덤 수열 발생기

[발명의 상세한 설명]

본 발명은 동일한 여러 개의 선형 궤환 쉬프트 레지스터를 사용하여 병렬 의사 랜덤 수열 발생기를 구성하는 경우 각 의사 랜덤 수열 발생기에 대하여 동작 상태를 실시간으로 확인하는 장치에 관한 것이다.

고속의 직렬 데이터를 랜덤한 이진 수열에 의해 스크램블링하는 경우, 데이터의 전송속도를 유지하면서 스크램블링을 하기 위해서는 스크램블링에 필요한 랜덤한 이진 수열을 생성하는 속도가 데이터의 전송속도와 동일하거나, 그 이상이어야 한다. 그러나 스크램블러로 흔히 사용되는 의사 랜덤 수열 발생기는 랜덤한 이진 수열을 생성하는 속도가 제한되어 있어서, 직렬 데이터를 병렬 데이터로 변환하고, 동일한 의사 랜덤 수열 발생기를 여러개 사용하여 랜덤한 이진 수열을 얻어 스크램블링을 한 다음, 다시 직렬 데이터로 변환하여 전송한다. 특히 비디오 데이터와 같은 데이터는 지연 시간에 의한 영향을 심하게 받으므로, 이를 최소화 하기 위해 전송속도가 빠른 채널을 요구하는 한편, 데이터를 직병렬 변환하여 단일 채널이 아닌 다중 채널을 이용하여 전송하는 경우가 있다. 이러한 경우 데이터의 스크램블링에는 동일한 의사 랜덤 수열 발생기를 이용한다. 이와 같이 여러 개의 동일한 의사 랜덤 수열 발생기를 사용하여 시스템을 구성할 경우 시스템의 신뢰도를 위하여 각 의사 랜덤 수열 발생기의 정상적인 동작상태를 수시로 확인하여야 한다. 그러나, 의사 랜덤 수열 발생기의 출력을 이용하여 데이터를 스크램블링하지 않고 있는 경우에는 의사 랜덤 수열 발생기에 특정한 초기치를 입력하고 출력되는 수열을 분석하므로써 가능하다. 의사 랜덤 수열 발생기의 출력을 이용하여 실시간으로 데이터를 스크램블링 하고 있는 경우에는 각 의사 랜덤 수열 발생기가 올바르게 동작을 하고 있는지 확인하는 것은 매우 어려운 일이다.

따라서, 본 발명에서는 상기의 문제점을 해결하여, 의사 랜덤 수열 발생기를 병렬로 사용하여 랜덤한 수열을 얻는 시스템에서 각 의사 랜덤 수열 발생기의 동작 상태를 실시간으로 확인하는 장치를 제공하는데 그 목적이 있다.

상기 목적을 달성하기 위하여 본 발명은, 다수개의 의사 랜덤 수열 발생기들의 출력 중 하나를 선택하는 선택수단, 상기 의사 랜덤 수열 발생기에서 사용된 외부 클럭을 입력받고, 외부의 제어 신호에 의해 마스크 벡터와, 초기치를 각각 입력받아 순차적으로 상기 다수개의 의사 랜덤 수열 발생기에서 발생하는 의사 랜덤 수열과 동일한 검사용 의사 랜덤 수열을 발생하는 검사용 의사 랜덤 수열 발생수단, 및 상기 선택수단에 의해 선택된 의사 랜덤 수열과 상기 검사용 의사 랜덤 수열 발생수단에 의해 발생한 의사 랜덤 수열을 비교하여, 그 결과를 출력하는 비교수단을 구비한 것을 특징으로 한다.

이하, 첨부된 도면을 참조하여 본 발명의 일 실시예를 상세히 설명한다.

제1도는 선형 궤환 쉬프트 레지스터로 구성된 의사 랜덤 수열 발생기를 병렬로 사용하는 시스템의 구성도로서, 본 발명은 이러한 시스템에서 각 의사 랜덤 수열 발생기의 동작 상태를 확인하는 장치에 관한 것이다. 그리고 도면에서 U106 내지 U110은 배타적논리합게이트(EX-OR), U101 내지 U105는 D플립플롭을 각각 나타낸다.

제2도는 의사 랜덤 수열 발생기를 병렬로 이용하는 병렬 스크램블러의 일예시도로, 각 의사 랜덤 수열 발생기(U201 내지 U206)는 제1도와 같은 구조를 갖는다.

제3도는 마스크 회로와 초기치 입력 회로가 부가된 선형 계한 쉬프트 레지스터로 검사용 의사 랜덤 수열 발생기의 상세 회로도이며, 제4도는 본 발명에 따른 병렬 의사 랜덤 수열 발생기의 동작 상태 확인 방법의 구성도이고, 제5도는 본 발명에 따른 병렬 의사 랜덤 수열 발생기의 동작 상태 확인 방법의 상세 회로도이다.

본 발명에 따른 병렬 의사 랜덤 수열 발생기에 대한 실시간 동작 확인장치는 제4도와 같이 여러개의 의사 랜덤 수열 발생기 출력 중 하나를 선택하는 입력 선택부(1), 검사용 수열을 발생하는 검사용 수열 발생기(2), 그리고 입력 선택부(1)에 의해 선택된 의사 랜덤 수열 발생기의 출력과 검사용 출력 발생부(2)에서 생성된 출력을 비교하는 검사 회로부(3)로 구성된다.

입력 선택부(1)는 제2도의 병렬 스크램블러에서 각 의사 랜덤 수열 발생기(U201~U203)의 출력을 입력으로 하여, 이들 입력 중 하나를 선택하여 출력한다.

검사용 수열 발생부(2)는 제3도에 도시된 검사용 의사 랜덤 수열 발생기와 동일한 회로로 구성된다. 즉, 이는 마스크 회로와 초기치 입력 회로가 부가된 선형계환 쉬프트 레지스터로 구성되어, 마스크 벡터에 의해 각 D플립플롭(U311~U314)의 출력(Q)을 마스크하여 검사에 필요한 비트를 출력한다.

검사 회로부(3)는 입력 선택부(1)에 의해 선택된 병렬 스크램블러의 출력과 검사용 수열 발생부(2)에 의

해 생성된 출력을 비교하여 검사 결과를 출력한다.

제5도에서 입력 선택부(1)는 제2도와 같이 의사 랜덤 수열 발생기를 병렬로 사용하는 경우 각 의사 랜덤 수열 발생기(U204~U206)의 출력( $Out_1 \sim Out_k$ )이 입력( $A_0 \sim A_{k-1}$ )으로 연결되고, 이진 계수기의 출력( $C_{out}$ )의 입력의 선택 순서를 결정하는 선택 입력(Select)으로 연결되며, 출력(0)이 배타적논리합게이트(U504)의 입력으로 연결되는  $k \times 1$ 의 멀티플렉서(MUX: U501)와, 외부 클럭이 클럭 입력(CLK)으로 연결되고, 계수 출력( $C_{out}$ )이 멀티플렉서(MUX: U501)의 선택 입력(Select)으로 연결되는 이진 계수기(U501)로 구성된다.

검사용 수열 발생기(2)는 제3도에 도시된 회로와 동일한 구조를 가지며, 외부 클럭이 클럭 입력(CLK)으로 연결되고, 출력(Sum)이 배타적논리합게이트(U504)의 입력으로 연결되며, 마스크 벡터 입력이 마스크 벡터 입력( $q_1 \sim q_2$ )으로 연결되고, 마스크 벡터 입력 제어 신호가 마스크 벡터 제어 입력(Latch)으로 연결되며, 초기치가 초기치 입력( $B_1 \sim B_n$ )으로 연결되고, 초기치 입력 제어신호가 초기치 제어신호 입력(S)으로 연결되는 검사용 의사 랜덤 수열 발생기(U503)로 구성된다.

검사 회로부(3)는 멀티플렉서(MUX)의 출력(0)과 검사용 의사 랜덤 수열 발생기(U503)의 출력(Sum)이 각각 입력으로 연결되고, 출력으로 검사 결과를 내어 놓는 배타적논리합게이트(U504)로 구성된다.

다음은 여러개의 의사 랜덤 수열 발생기(U201~U203)를 사용하여 병렬 스크램블링하는 일예와 각 의사 랜덤 수열 발생기(U201~U203)의 출력( $Out_1 \sim Out_k$ )과 동일한 출력 수열을 생성하기 위해 검사용 의사 랜덤 수열 발생기(U503)를 마스크하는 방법에 대하여 설명한다.

제1도의 선형 궤환 쉬프트 레지스터를 구성되는 의사 랜덤 수열 발생기 K개를 제2도와 같이 병렬로 연결하여 스크램블링하는 경우 각 의사 랜덤 수열 발생기의 출력 수열은  $(s-1)(2^n/k)+i$ ,  $i=1, 2, 3, \dots, s=1, 2, 3, \dots, k$ 의 순서로 나타나야만 출력 수열이 주기 내에서 서로 중복되지 않고 나타날 수 있다. 일 예로써, 의사 랜덤 수열 발생기를 구성하는 원시 다항식이  $f(x)=x^5+x^2+1$ 이라 하고, 4개의 의사 랜덤 수열 발생기를 사용하여 병렬 스크램블링 할 경우  $k=4$ 가 된다. 제2도에서 의사 랜덤 수열 발생기 1은  $s$ 가 1이므로 1, 2, 3, 4, 5, ... 번째의 출력 수열이 나타나고, 의사 랜덤 수열 발생기 2는  $s$ 가 2이므로 9, 10, 11, 12, 13, ... 번째의 출력 수열이 나타나며, 의사 랜덤 수열 발생기 3은  $s$ 가 3이므로 17, 18, 19, 20, 21, ... 번째의 출력 수열이 나타나고, 마지막 의사 랜덤 수열 발생기 4는  $s$ 가 4이므로 25, 26, 27, 28, 29, ... 번째의 출력 수열이 나타나게 된다. 따라서 첫 번째 의사 랜덤 수열 발생기를 구성하는 레지스터들의 초기치는 1이고, 두 번째 의사 랜덤 수열 발생기를 구성하는 레지스터들의 초기치는 1101이며, 세 번째 의사 랜덤 수열 발생기를 구성하는 레지스터들의 초기치는 1111이고, 네 번째 의사 랜덤 수열 발생기를 구성하는 레지스터들의 초기치는 1101이다. 각 의사 랜덤 수열 발생기의 출력을 정리하면 다음과 같다.

출력순서(입력되는 클럭) : 1 2 3 4 5 6 7 8

의사 랜덤 수열 발생기 1의 출력 수열 : 0 0 0 0 1 0 1 0

주기 내에서의 출력 순서 : 1 2 3 4 5 6 7 8

의사 랜덤 수열 발생기 2의 출력 수열 : 1 1 1 0 1 1 0 0

주기 내에서의 출력 순서 : 9 10 11 12 13 14 15 16

의사 랜덤 수열 발생기 3의 출력 수열 : 0 1 1 1 1 1 0 0

주기내에서의 출력 순서 : 1 7 18 19 20 21 22 23 24

의사 랜덤 수열 발생기 4의 출력 수열 : 1 1 0 1 0 0 1 0

주기 내에서의 출력 순서 : 25 26 27 28 29 30 31 32

이상에서 각 의사 랜덤 수열 발생기에 입력되는 클럭을 나타내는 주기내의 출력 순서는 각 의사 랜덤 수열 발생기의 출력 수열이 주기내에서 위치하는 순서를 나타낸다. 상기 의사 랜덤 수열 발생기의 출력 수열을 검사하기 위해 검사용 의사 랜덤 수열 발생기는 첫 번째 클럭에 의해서는 첫 번째 의사 랜덤 수열 발생기의 출력 수열과 동일한 수열을 발생시켜야 하고, 두 번째 클럭에 의해서는 두 번째 의사 랜덤 수열 발생기의 출력 수열과 동일한 수열을 발생시켜야 하며, 네 번째 클럭에 의해서는 네 번째 의사 랜덤 수열 발생기의 출력 수열과 동일한 수열을 발생시켜야 하고, 다섯 번째 클럭에 의해서는 다시 첫 번째 의사 랜덤 수열 발생기의 출력 수열과 동일한 수열을 발생시켜야 한다. 이와 같이 클럭 순서에 따라 쉬프트되며 각 의사 랜덤 수열 발생기의 출력과 동일한 수열을 발생시켜야 한다. 따라서 검사용 의사 랜덤 수열 발생기의 출력 수열이 다음과 같다면 각 의사 랜덤 수열 발생기 출력과 비교함으로써 실시간 확인이 가능하다. 이때 검사용 의사 랜덤 수열 발생기를 구성하는 레지스터의 초기치는 첫 번째 의사 랜덤 수열 발생기를 구성하는 레지스터의 초기치와 동일하여야 하며, 검사용 의사 랜덤 수열 발생기의 출력 수열을 정리하면 다음과 같다.

출력 순서(입력되는 클럭) : 1 2 3 4 5 6 7 8

검사용 의사 랜덤 수열 발생기의 출력 수열 : 0 1 1 1 1 1 0 0

주기 내에서의 출력 순서 : 1 10 19 28 5 14 23 32

선형 궤환 쉬프트 레지스터에 의해 구성되는 의사 랜덤 수열을 발생기의 출력을 일정한 순서로 샘플링하는 방법에 의해 구성하면 전체 주기의 출력 수열과 동일한 성질을 가지고 있다. 따라서 검사용 의사 랜덤 수열 발생기의 출력 수열을 새로이 정리하면 다음과 같다.

출력 순서(입력되는 클럭) : 1 2 3 4 5 6 7 8

검사용 의사 랜덤 수열 발생기의 출력 수열 : 0 1 1 1 1 1 0 0

주기 내에서의 출력 순서 : 17 18 19 20 21 22 23 24

이와 같이 주기 내의 출력 순서를 연속적인 순서로 재배열 한 것은 마스크 벡터를 쉽게 구하기 위해서이다. 의사 랜덤 수열 발생기를 구성하는 선형 계환 쉬프트 레지스터를 구성하는 원시 다항식을  $f(x)$ 라 하고 마스크 벡터를 표현하는 다항식을  $q(x)$ 라 하면, 마스크 벡터를 구하기 위한 식은 다음과 같다.

$$q(x) = x^{(L-p+n)} \text{ modulo } f(x)$$

여기서  $L$ 은 의사 랜덤 수열 발생기를 구성하는 선형 계환 쉬프트 레지스터의 주기,  $P$ 는 주기내의 출력 수열 중 제일 처음 나타나는 순서,  $n$ 은 차수를 나타낸다. 위에서 예로 들은 경우 검사용 의사 랜덤 수열 발생기의 마스크 벡터는  $x^{19} \text{ modulo } (x^5 + x^2 + 1) = x^2 + x$ 가 되어  $\{0, 0, 1, 1, 0\}$ 이 된다. 이상의 마스크 벡터들은 제2도의 마스크 벡터 입력  $\{q_n, \dots, q_{2q_1}\}$ 의 순서로 대응된다.

회로의 동작은 이상에서 예시한 방법에 준하여 설명한다.

제5도에서 이상에서 설명한 바와 같이 계산된 마스크 벡터를 마스크 벡터 입력( $q_1 \sim q_n$ )에 입력하고, 마스크 벡터 입력 제어 신호를 토글링하면 마스크 벡터는  $n$ 비트 래치(U341)에 저장되어 D플립플롭(U311~U314)의 출력을 마스크한다. 초기치는 제2도에서 사용된 병렬의사 랜덤 수열 발생기 중 의사 랜덤 수열 발생기 I(U201)의 초기치 위에서 예로들은 경우 1을 초기치 입력( $B_1 \sim B_n$ )으로 하여 초기치 입력 제어신호를 토글링 하면 D플립플롭(U311~U314)의 초기치로 입력된다. 이처럼 입력된 마스크 벡터와 초기치에 의해 외부 클럭을 입력으로 하여 병렬로 사용된 의사랜덤 수열 발생기의 출력 중 일부를 순차적으로 발생하게 된다. 이진 계수기(U205)의 출력( $C_{out}$ )은 랜덤 수열 발생기를 4개 사용하는 경우 2비트 출력이 되어 0, 1, 10, 11 즉, 0, 1, 2, 3을 계속 반복하여 출력하며, 이 출력( $C_{out}$ )을 선택 입력(Select)으로 하는  $k \times 1$  MUX(U501)는 4개의 의사 랜덤 수열 발생기(제2도의 U201~U203)의 출력( $Out_1 \sim Out_k$ )을 입력으로 하는 입력( $A_0 \sim A_3$ )을 출력(0)으로 내어 놓게 된다. 즉, 이진 계수기(U205)의 출력( $C_{out}$ )이 0인 경우에는  $k \times 1$  MUX(U501)는  $A_0$ 에 입력되는 의사랜덤 수열 발생기의 출력( $Out_1$ )을, 이진 계수기(U205)의 출력( $C_{out}$ )이 1인 경우에는  $k \times 1$  MUX(U501)는  $A_2$ 에 입력되는 의사 랜덤 수열 발생기의 출력( $Out_4$ )을 출력(0)으로 내어 놓는다. 그리고 검사용 의사 랜덤 수열 발생기는 이진 계수기(U205)의 출력( $C_{out}$ )이 0인 경우에는  $k \times 1$  MUX(U501)의  $A_0$ 에 입력되는 의사 랜덤 수열 발생기의 출력( $Out_1$ )과 동일한 출력 수열을 발생하고, 이진 계수기(U205)의 출력( $C_{out}$ )이 1인 경우에는  $k \times 1$  MUX(U501)의  $A_1$ 에 입력되는 의사랜덤 수열 발생기의 출력( $Out_2$ )과 동일한 출력 수열을 발생하며, 마찬가지로, 이진 계수기(U205)의 출력( $C_{out}$ )이 2인 경우에는  $k \times 1$  MUX(U501)의  $A_2$ 에 입력되는 의사 랜덤 수열 발생기의 출력( $Out_3$ )과 동일한 출력 수열을 발생하고, 이진 계수기의 출력( $C_{out}$ )이 3인 경우에는  $k \times 1$  MUX(U501)의  $A_3$ 에 입력되는 의사랜덤 수열 발생기의 출력( $Out_4$ )과 동일한 출력 수열을 발생한다.

멀티플렉서(MUX: U501)의 출력(0)과 검사용 의사 랜덤 수열 발생기(U503)의 출력(Sum)은 배타적논리합 게이트(U504)에 의해 비교되어, 두 입력이 동일한 경우에는 0을, 다른 경우에는 1을 출력하으로써, 병렬 의사 랜덤 수열 발생기의 출력 수열을 실시간으로 검증할 수 있다.

따라서, 상기와 같이 구성되어 동작하는 본 발명은, 동일한 의사 랜덤 수열 발생기를 사용하여 출력된 수열을 사용하는 시스템의 동작 상태를 실시간으로 확인할 수 있으므로, 시스템의 신뢰도를 높일 수 있다.

## (57) 청구의 범위

### 청구항 1

다수개의 의사 랜덤 수열 발생기들의 출력 중 하나를 선택하는 선택수단, 상기 의사 랜덤 수열 발생기에서 사용된 외부 클럭을 입력받고, 외부의 제어 신호에 의한 마스크 벡터와, 초기치를 각각 입력받아 순차적으로 상기 다수개의 의사 랜덤 수열 발생기에서 발생하는 의사 랜덤 수열과 동일한 검사용 의사 랜덤 수열을 발생하는 검사용 의사 랜덤 수열 발생수단, 및 상기 선택수단에 의해 선택된 의사 랜덤 수열과 상기 검사용 의사 랜덤 수열 발생수단에 의해 발생된 의사 랜덤 수열을 비교하여, 그 결과를 출력하는 비교수단을 구비하는 병렬 의사 랜덤 수열 발생기에 대한 실시간 동작 확인장치.

### 청구항 2

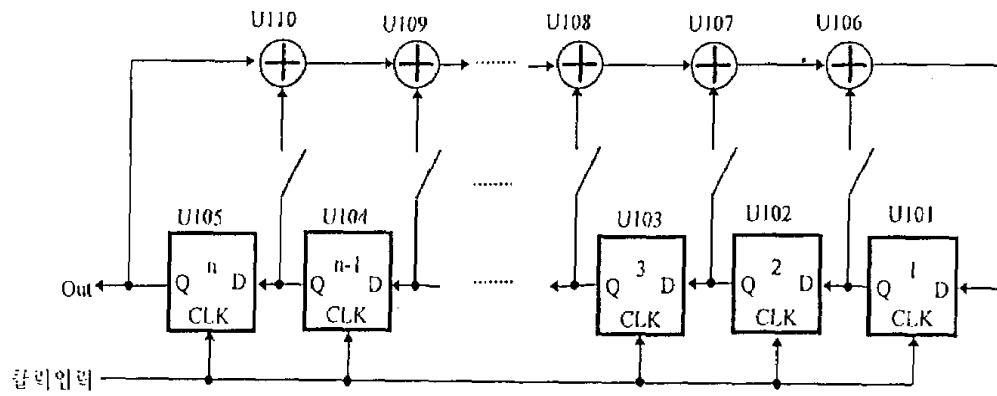
제1항에 있어서, 상기 선택수단은, 상기 의사 랜덤 수열 발생기에서 사용된 외부 클럭을 입력받아 상기 클럭에 따라 카운트 값을 발생하는 계수수단, 및 상기 계수수단에 의해 발생된 카운트 값에 따라 상기 다수개의 의사 랜덤 수열 발생기로부터 입력된 의사 랜덤 수열들 중 하나를 선택하여 출력하는 멀티플렉서를 구비한 것을 특징으로 하는 병렬 의사 랜덤 수열 발생기에 대한 실시간 동작 확인 장치.

### 청구항 3

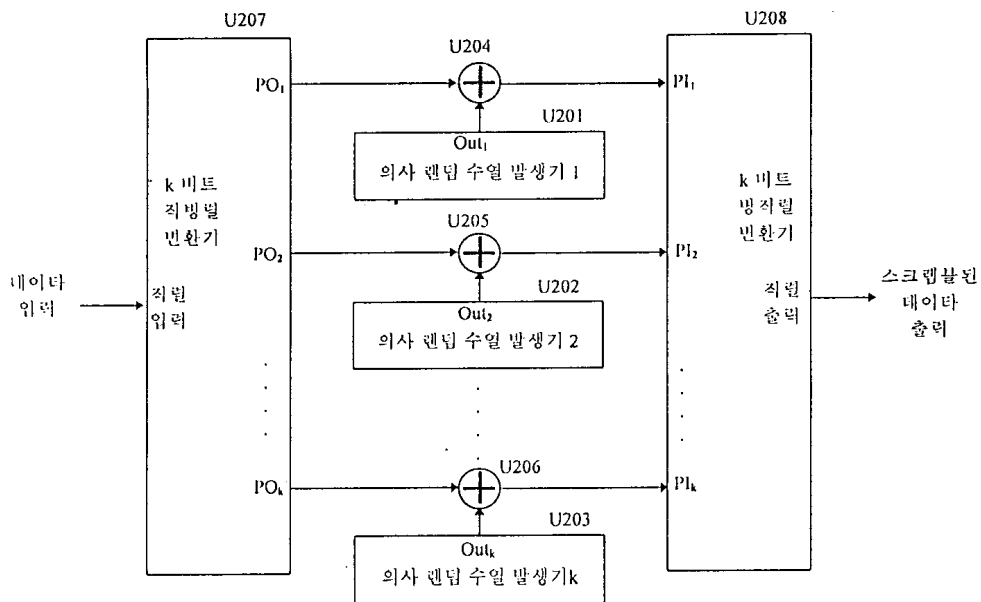
제2항에 있어서, 상기 비교수단은, 상기 멀티플렉서의 출력과 상기 검사용 의사 랜덤 수열 발생수단의 출력을 배타적 논리합하는 배타적 논리합 게이트를 포함한 것을 특징으로 하는 병렬 의사 랜덤 수열 발생기에 대한 실시간 동작 확인장치.

## 도면

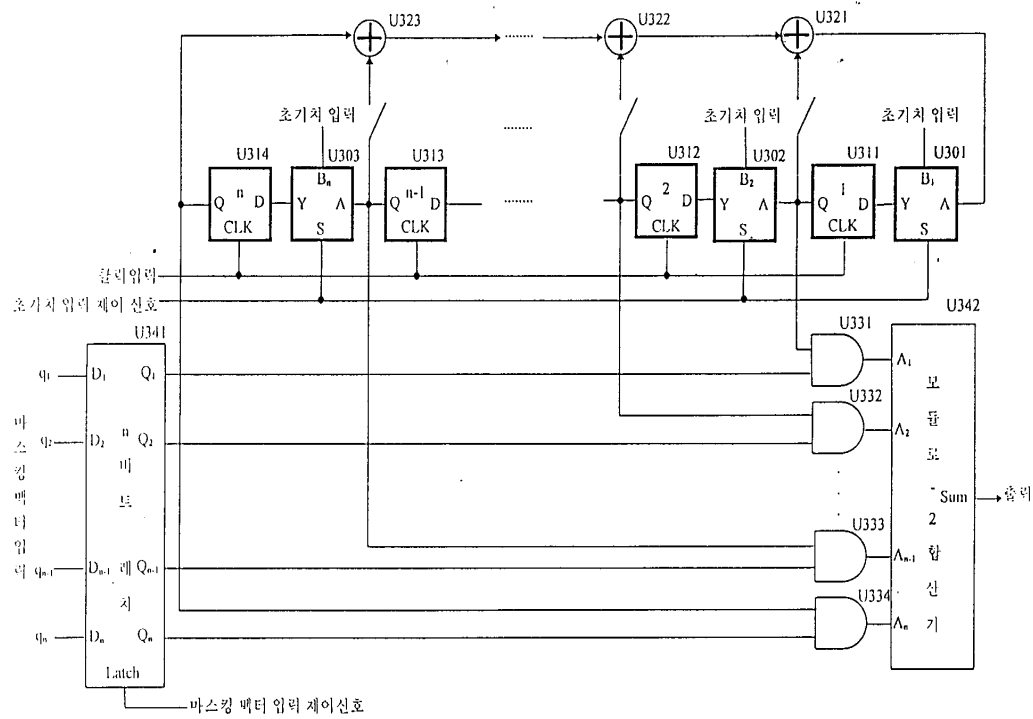
도면1



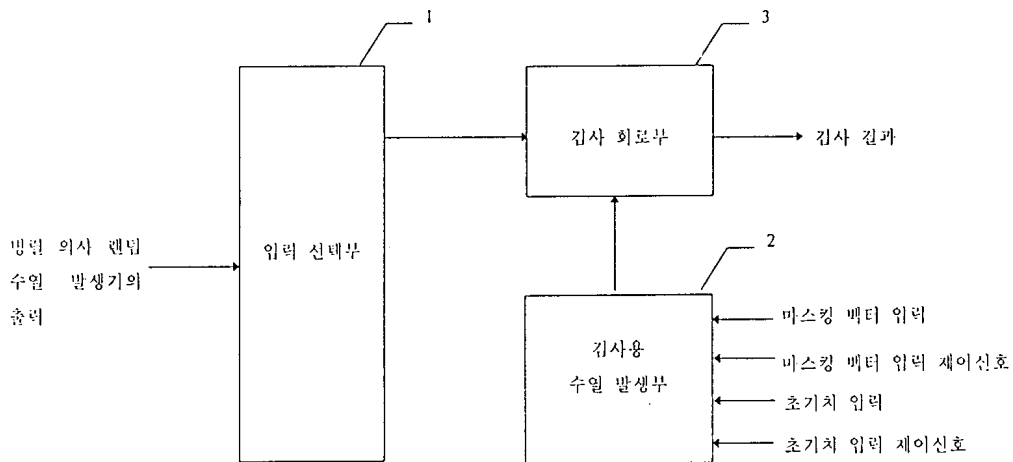
도면2



도면3



도면4



도면5

