(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.
G06F 7/58 (2006.01)

(45) 공고일자 2006년04월28일
(11) 등록번호 10-0574730
(24) 등록일자 2006년04월21일

(21) 출원번호 10-2002-0058111
(22) 출원일자 2002년09월25일

(65) 공개번호 10-2003-0027724
(43) 공개일자 2003년04월07일

(30) 우선권주장 JP-P-2001-00294836 2001년09월26일 일본(JP)
JP-P-2002-00183967 2002년06월25일 일본(JP)

(73) 특허권자 가부시끼가이샤 도시바
일본국 도꾜도 미나또꾸 시바우라 1쪼메 1방 1고

(72) 발명자 후지따시노부
일본가나가와껭가와사끼시사이와이꾸고무까이도시바쪼1가부시끼가이샤도시바리써치앤드디벨롭먼트센터내

우찌다겐
일본가나가와껭요꼬하마시이소고꾸신스기따쪼8가부시끼가이샤도시바요꼬하마퍼실러티어드미니스트레이션센터내

오바류지
일본가나가와껭요꼬하마시이소고꾸신스기따쪼8가부시끼가이샤도시바요꼬하마퍼실러티어드미니스트레이션센터내

고가준지
일본가나가와껭요꼬하마시이소고꾸신스기따쪼8가부시끼가이샤도시바요꼬하마퍼실러티어드미니스트레이션센터내

(74) 대리인 장수길
구영창

심사관 : 성경아

(54) 난수 발생 회로

요약

본 발명의 난수 발생 회로는 무작위도가 높은 난수를 발생할 수 있으며, 소형의 집적 회로로서 구성될 수 있다. 본 발명의 난수 발생 회로는 디지탈 입력값에 의해 일의적으로 결정되지 않은 디지탈 출력값을 제공하는 플립플롭형 논리 회로를 갖는 불확정 논리 회로와, 불확정 논리 회로로부터의 디지탈 출력값에서 "0"과 "1"의 출현 빈도를 동일하게 하는 등화 회로를 포함한다.

대표도

도 1

색인어

플립플롭 논리 회로, 피드백 시프트 레지스터, XOR 연산, XOR 회로, NAND 회로

명세서

도면의 간단한 설명

도 1은 본 발명의 실시예에 따른 난수 발생 회로의 기본 부분의 구성을 도시하고 있는 블록도.

도 2는 본 발명의 실시예에 따른 난수 발생 회로의 기본적인 구성을 도시하고 있는 개략도.

도 3은 본 발명의 제1 실시예에 사용된 RS-FF(10A)의 특정 구성을 도시하고 있는 개략도.

도 4는 RS-FF의 동작을 나타내는 펄스를 도시하고 있는 도면.

도 5는 2개의 NOR 논리 회로(11, 12)가 접속되어 있는 RS-FF의 다른 특정 예를 도시하고 있는 개략도.

도 6은 도 5에 도시된 RS-FF의 동작을 설명하기 위한 펄스를 도시하고 있는 도면.

도 7은 본 발명의 실시예에 따른 난수 발생 회로의 불확정 논리 회로(10)의 기본 부분을 도시하고 있는 개략도.

도 8a 및 도 8b는 본 발명의 실시예에 따른 플립플롭 회로의 동작을 도시하고 있는 개략도.

도 9는 본 발명의 실시예에서의 등화 회로의 동작의 개념을 설명하는 도면.

도 10은 등화 회로의 다른 특정 예를 도시하고 있는 개략도.

도 11은 등화 회로의 다른 특정 예를 도시하고 있는 개략도.

도 12는 2개의 플립플롭을 사용하는 다른 특정 예를 도시하고 있는 개략도.

도 13은 본 발명의 실시예에 따른 난수 발생 회로의 기본 부분의 구성을 도시하고 있는 개략도.

도 14a 및 도 14b는 본 발명의 제5 실시예의 구성에 대한 개념을 도시하고 있는 개략도.

도 15a 및 도 15b는 본 발명의 제5 실시예의 기본 부분의 구성을 도시하고 있는 개략도.

도 16은 랜덤 입력의 방법으로서 주파수가 상이한 비동기식 발진기 회로를 사용하는 구성을 도시하고 있는 개략도.

도 17은 의사 난수를 발생할 수 있는 선형 피드백 시프트 레지스터 LSFR(Linear Feedback Shift Register)를 사용하여 시프트 레지스터 SR 중의 하나로부터 랜덤 입력을 인입(invite)하는 구성을 도시하고 있는 개략도.

도 18a 및 도 18b는 본 발명의 제6 실시예에 따른 회로의 기본 부분을 도시하고 있는 개략도.

도 19는 UFF에 입력되는 펄스 전압에 대한 "1"의 출현 확률의 의존도를 도시하고 있는 그래프.

<도면의 주요 부분에 대한 부호의 설명>

10 : 불확정 논리 회로

10A~10C : RS-형 플립플롭

11, 12 : NOR 회로

13, 14 : MOS 트랜지스터

20 : 등화 회로

20A : XOR 회로

20B : T형 플립플롭

20C : FSR

20D : 카운터

20E : 피드백 회로

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 출원은 2001년 9월 26일자로 출원된 종래 일본 특허 출원 제2001-294836호, 및 2002년 6월 25일자로 출원된 종래 일본 특허 출원 제2002-183967호의 우선권에 기초하여 그 이점을 청구한다. 이들 전체 내용은 참조로서 본원에 포함된다.
본 발명은 난수 발생 회로에 관한 것으로, 보다 구체적으로는 디지탈 논리 회로를 이용하여 소형으로 구성 가능하고, 높은 무작위도(randomness)로 난수를 발생할 수 있으며, 암호화 알고리듬에 사용하기에 적합한 난수 발생 회로에 관한 것이다.

디지탈 난수는 예를 들어 확률 처리에 의해 수반되는 현상의 시뮬레이션 및 보안을 목적으로 하는 암호화 알고리듬을 위한 암호키, 식별 번호 및 패스워드의 생성 처리에 사용된다. 종래의 기술은 디지탈 난수로서 CPU에 의한 연산으로 작성된 의사 디지탈 숫자(pseudo digital number)를 사용하여 왔다. 이러한 의사 난수(pseudo random number)는 통상적으로 피드백 시프트 레지스터(feedback shift register)로 지칭되는 논리 회로로 작성되었다.

한편, 저항 또는 다이오드에서 발생된 잡음을 사용하여 난수를 작성하는 방법도 실제로 사용되어 왔다. 이 방법에서는 랜덤한 숫자에서 불균일성(unevenness) 또는 주기성(periodcity)이 제거되며, 거의 "신뢰할 수 있는 난수"가 얻어질 수 있다. 이 유형의 난수 발생 회로는 잡음 소스의 요소에 정전류를 흐르게 하여 잡음을 발생시키고, 그 잡음을 고역 통과 필터에 제공하여 AC 성분을 추출하며, 이 AC 성분을 아날로그 회로에서 증폭시킨 후 AD 변환에 의해 디지탈값으로 변환한다. 이 때, 특정값을 임계값으로 하여, 임계값을 초과하는 AC 성분을 "1"로 결정하고, 임계값에 도달하지 못하는 AC 성분을 "0"으로 결정한다. 더욱이, 획득된 난수 시퀀스가 불균일성을 나타내기 때문에 대부분의 경우 디지탈 회로에 의한 보정 후에 사용된다.

이미 공지된 바와 같이, CPU에 의해 작성된 의사 난수는 초기에 동일한 숫자(씨드)가 주어진다면 똑같은 난수가 되며, 이들 의사 난수가 레지스터의 숫자에 기초한 주기성을 가져 바람직하지 않기 때문에 난수로서 적합하지 않다. 특히, 보안에 사용하는 경우, 이들은 "암호키"가 깨질 가능성을 갖는다.

한편, 저항 및 다이오드의 열잡음과 산탄 잡음(shot noise)이 통상 아날로그 신호이고 그들의 출력이 작기 때문에, 잡음을 증폭하도록 구성된 유형의 회로는 대규모 아날로그 앰프 회로(a large-scaled analog amplifier circuit)를 필요로 하여 집적 및 소형화가 곤란하다. 특히, IC 카드 등의 암호 보안 기능을 위한 소형 장치에 통합시키기가 용이하지 않다.

따라서, 어떠한 주기성도 없이 고품질 난수를 발생할 수 있는 소형 집적 회로가 요구되고 있다.

소형화를 위해서는 회로가 예를 들어 TTL 혹은 MOS 등의 디지탈 회로의 형태로 구성되는 것이 바람직하다. 그러나, 디지탈 회로는 기본적으로 특정 입력에 응답하여 동일한 출력을 생성하기 때문에 알고리듬 처리에 의한 난수를 작성할 수 있을 뿐이다. 따라서, 피드백 시프트 레지스터와 마찬가지로 의사 난수를 작성할 수 있을 뿐이다.

이러한 단점을 해소하기 위해서는 특정되지 않은 출력을 생성할 수 있는 디지탈 회로를 구성하는 것이 필요하다.

발명이 이루고자 하는 기술적 과제

본 발명의 특징에 따르면, 디지탈 입력값에 의해 일의적으로 결정되지 않은 디지탈 출력값을 제공하는 플립플롭형 논리 회로를 포함하는 불확정 논리 회로와, 상기 불확정 논리 회로로부터의 상기 디지탈 출력값에서 "0"과 "1"의 출현 빈도를 동일하게 하는 등화 회로를 구비하는 난수 발생 회로가 제공된다.

발명의 구성 및 작용

본 발명의 실시예에 대한 상세한 설명과 첨부 도면을 참조하여 본 발명을 더욱 구체적으로 설명할 것이다. 그러나, 첨부 도면은 본 발명을 특정한 실시예로 제한하기 위한 것이 아니라 단지 설명과 예시를 통한 이해를 돕기 위한 것이라는 점에 유의하기 바란다.

본 발명의 실시예를 도면을 참조하여 상세히 설명한다.

도 1은 본 발명의 실시예에 따른 난수 발생 회로의 기본 부분의 구성을 도시하고 있는 블록도이다.

실시예에 따른 난수 발생 회로는 불확정 논리 회로(10)와 이 불확정 논리 회로(10)에 의해 입력이 공급되는 등화 회로(20)를 포함한다.

불확정 논리 회로(10)는 디지탈 회로 형태의 논리 회로이다. 불확정 논리 회로의 원리는 출력 "0" 또는 "1"이 입력 신호의 특수한 조합에 대해 불확정하게 된다는 점이다. 논리 회로가 불확정인 경우, 출력이 논리 회로(10)의 구성요소의 시시각각의 물리적인 요소에 따라 변화한다. 이 물리적인 현상을 이용함으로써, 일정 입력을 갖는 경우에도 출력이 변화하는 디지탈 회로를 얻을 수 있고, 디지탈 신호 "0"과 "1"의 랜덤 시퀀스를 얻을 수 있다.

이 방법에 의해 획득된 시퀀스에서의 디지탈 신호 "0"과 "1"의 순서가 디지탈 회로의 구성요소의 특성에 좌우되기 때문에, "0"과 "1"의 출현 빈도에서 "불균일성"이 발생된다.

그러므로, 등화 회로(20)는 디지탈 신호의 추가의 디지탈 처리를 수행하여 불균일성을 제거하고 무작위도가 높은 디지탈 난수를 얻게 된다. 이와 달리, 피드백 루프 F로서 도 1에 예시된 바와 같이, 등화 회로(20)는 불확정 논리 회로(10)의 출력 데이타에 기초한 피드백 신호를 불확정 논리 회로(10)에 공급하여 출력 데이타에서의 "불균일성"을 제거하도록 구성될 수도 있다.

이 방식에서, 난수 발생 회로는 더 적은 수의 논리 게이트로 구성될 수 있고, 그에 따라 소형 회로로 설계될 수 있다. 또한, "0"과 "1"의 빈도를 정정하기 위한 회로도 상당히 콤팩트한 논리 회로로 형성될 수 있다.

난수의 원인이 되는 현상이 불확정 논리 회로(10)의 각각의 구성요소의 물리적인 현상에 기초하기 때문에, 똑같은 입력에 응답하여 불확정한 출력이 획득될 수 있다. 따라서, 난수 시퀀스는 주기성을 나타내지 않으며, 난수의 추정(estimation of random number)이 가능한 의사 난수와는 상이한 고품질 난수가 획득될 수 있다.

이하에서는 특정 예를 참조하여 본 발명의 실시예를 더욱 구체적으로 설명한다.

(제1 실시예)

도 2는 본 발명의 실시예에 따른 난수 발생 회로의 기본 구성을 도시하고 있는 개략도이다.

도 2에 도시된 난수 발생 회로는 불확정 회로(10)내에 RS(리셋-세트)형 플립플롭(RS-FF)(10A)을 포함한다.

도 3은 본 발명의 제1 실시예에 사용된 RS-FF(10A)의 특정 구성을 도시하고 있는 개략도이다. 도시된 바와 같이, RS-FF(10A)는 2개의 NOR 논리 회로(11, 12)의 조합으로 이루어진다.

입력이 S=R=0 인 경우, 대응 출력 Q는 이전의 플립플롭 출력 Q와 동일한 값이 된다. 그러나, 이전의 상태가 파워-오프 상태라면, 후속의 파워-온 상태 후의 출력은 불확정하게 된다. S=R=0가 실제로 입력될 때, 출력은 NOR 회로(11, 12)를 형성하는 복수의 CMOS의 턴온 타이밍간의 미묘한 차이에 따라 "0" 또는 "1"로 결정된다. 특성의 미묘한 차이가 항상 일정한 것은 아니며, 그보다는 회로의 주변 부품의 온도, 회로에서 물리적으로 발생된 작은 잡음 등에 의해 결정된다. 따라서, 출력도 마찬가지로 일정하지 않다.

도 4는 RS-FF의 동작을 나타내는 펄스를 도시하고 있는 도면이다.

여기서, S=R=0를 유지하면서 맥동 방식(pulsating manner)에서의 NOR 회로(11, 12)의 전원 전압 Vcc(Vin)의 온과 오프가 각각 입력 "0"와 "1"인 것으로 가정한다. 플립플롭의 정보를 완전하게 소거하기에 충분한 지속기간 동안 "0"를 입력한 후에 "1"을 입력함으로써 플립플롭의 출력이 불확정으로 된다면, 입력 "1"에 응답하여 불확정 출력 Q가 획득된다. 따라서, 입력으로 "0"과 "1"을 반복함으로써, "0" 또는 "1"의 수치값의 불확정하고 랜덤한 시퀀스가 도 4에 도시된 바와 같이 출력 Q로서 획득될 수 있다.

그러나, 논리 회로(11, 12)를 형성하는 트랜지스터가 절대적으로 대칭적인 것은 아니기 때문에, "0"의 출현 빈도와 "1"의 출현 빈도는 동일하지 않아 "0"과 "1" 중의 하나가 다른 하나보다 더 빈번하게 출현한다. 따라서, 후술되는 바와 같이, 본 실시예에 따른 난수 발생 회로를 형성하기 위해 출현 빈도에 있어서 "0"과 "1"을 동일하게 하기 위한 회로(20)가 결합된다.

인버터의 구성을 갖는 디지탈 회로를 사용하여 디지탈 난수를 발생하는 방법이 있다. 이 방법은 예를 들어 일본 특허 공개 공보 2001-166920호에 개시된 바와 같은 디지탈 회로에 추가된 구성요소의 온도 변동(fluctuation)을 이용한다. 그러나, 이 종래의 기술에서는 홀수개의 인버터를 환형 모양으로 접속시킴으로써 구성된 링 발진기의 발진 주파수가 온도에 따라 불안정하게 되며, 이것은 본 발명과는 완전히 상이하다. 또한, 이 종래 기술은 전체 구성이 복잡하고 회로 크기도 크며, 이러한 점에서도 개량의 여지가 있다. 더욱이, 링 발진기와 같은 정궤환 방식의 발진기 회로의 경우에, 발진을 개시하기 위한 트리거가 회로의 기본 클록과 동기하는 잡음 신호이며, 발진기 회로와 클록은 절대로 비동기될 수 없다. 따라서, 발생된 난수 시퀀스에서 주기성이 나타나게 되어 난수의 무작위도를 저하시킨다.

반대로, 본 발명의 실시예는 플립플롭의 불확정 출력을 긍정적으로 생성함으로써 더더욱 콤팩트한 회로를 가지고 랜덤한 디지탈 신호 시퀀스를 효율적으로 획득할 수 있다.

본 실시예에서 RS형 플립플롭을 사용하는 경우에는 도 5에 도시된 바와 같이 2개의 NOR 논리 회로(11, 12)를 접속시킴으로써 전술된 특정 예와는 상이한 방식으로 불확정 출력이 획득될 수 있다.

도 6은 그 동작을 설명하기 위한 펄스를 나타내고 있는 도면이다.

이 경우, 전원 Vcc를 변함없이 온 상태로 유지하고 S=R을 입력으로 하는 동안, 도 6에 도시된 바와 같이 "1"과 "0"이 반복적으로 입력된다. S=R=0의 경우, 출력 Q는 이전 상태의 Q를 유지하고 출력 /Q(반전된 Q를 나타냄)는 이전 상태의 Q를 유지하여, 이들은 각각 "0"과 "1"을 취한다.

그러나, S=R=1의 경우, Q와 /Q는 동일하게 Q=0과 /Q=0가 된다. 따라서, 다음에 입력이 S=R=0가 될 때, 1 또는 0가 Q로 출현하게 되는 불확정이 된다. 그 결과, 도 6에 도시된 바와 같은 불확정 디지탈 신호 시퀀스가 획득된다.

그러나, 여기에서 획득된 디지탈 신호 시퀀스에서도, 대부분의 경우 "0"과 "1"의 출현 빈도가 동등하지 않다. 그러므로, "0"과 "1"의 출현 빈도를 동일하게 하기 위한 회로(20)가 결합되어 본 발명의 실시예에 따른 난수 발생 회로가 얻어진다.

본 실시예에 따른 난수 발생 회로의 블특정 논리 회로(10)는 다른 유형의 플립플롭을 사용하여 난수 발생 회로를 유사하게 구성함으로써 도 2 내지 도 6에 도시된 특정 예와 상이하게 구성될 수도 있다. 즉, D형 플립플롭의 경우에 클록 입력을 "0"로 설정하거나, JK 플립플롭의 경우에 클록 입력을 J=K=1 또는 0로 설정하거나, T형의 경우에 입력 T를 임의의 값으로 설정함으로써, 플립플롭의 초기값이 결정되지 않은 때에 출력은 불확정이 된다.

(제2 실시예)

다음으로 본 발명의 제2 실시예를 설명한다.

도 7은 본 발명에 따른 난수 발생 회로의 불확정 논리 회로(10)의 기본 부분을 도시하고 있는 개략도이다.

본 실시예에서, 불확정 논리 회로는 2개의 CMOS 회로(13, 14)의 구성을 갖고 이들의 게이트와 CMOS 트랜지스터를 접속시킨 플립플롭 회로(10C)를 포함한다. 이 플립플롭에서, MOS 트랜지스터 T1이 턴온될 때, MOS 트랜지스터 T3는 턴오프된다.

도 8은 도 7에 도시된 플립플롭 회로의 동작을 도시하고 있는 개략도이다.

전원이 오프일 때, 모든 트랜지스터는 오프 상태이고, 모든 전극의 전위는 접지 전위와 같게 된다.

Vin이 1(H: 하이)로 설정될 때, 각각의 트랜지스터의 게이트의 전위가 0(L: 로우)이기 때문에, 트랜지스터 T1과 트랜지스터 T3는 턴온될 수 있다. 그러나, 회로가 플립플롭이기 때문에, 이들 트랜지스터 중의 하나만이 턴온된다.

여기서 트랜지스터 T1이 도 8a에 도시된 바와 같이 먼저 턴온된다고 가정한다. 그러면, 트랜지스터 T1의 소스와 드레인은 도통 상태가 되고 전위가 동일하게 되며, A 지점에서의 전위는 Vin과 동일한 하이 레벨이 된다. 그 결과, 트랜지스터 T3는 턴오프되고, 트랜지스터 T4는 턴온되어 회로를 안정화시킨다. 이 때, B 지점, 즉 출력단에서의 전위는 초기 레벨인 로우 레벨(0)을 유지한다.

반대로, 트랜지스터 T3가 먼저 턴온된다고 가정하면, 회로는 도 8b에 도시된 바와 같이 되며, 출력은 하이 레벨(1)이 된다.

이와 같이, 트랜지스터 T1과 T3 중의 어느 것이 먼저 턴온되느냐에 따라 출력이 결정된다. 어느 트랜지스터가 먼저 턴온되는지는 특정되지 않으며, 회로는 이미 설명된 제1 실시예와 유사하게 출력이 불확정인 플립플롭으로서 기능한다. 플립플롭의 전원의 온과 오프 동작이 각각 디지탈 입력 "0"과 "1"로서 사용될 때, 회로는 입력 "1"에 응답하여 "0" 또는 "1"이 될 수도 있는 불확정 출력을 내보낸다.

그러나, 2개의 CMOS가 속성에 있어서 절대적으로 동일하지는 않고, T1과 T3 중의 어느 것이 먼저 턴온되느냐에 관한 불균일성이 존재한다. 그러나, 상세히 후술되는 바와 같이 등화 회로(20)를 이용하여 이를 보정함으로써, 무작위도가 높은 디지탈 숫자가 획득될 수 있다.

(제3 실시예)

다음에는 본 발명의 제3 실시예로 등화 회로(20)의 특정 예를 상세하게 설명한다.

전술된 제1 및 제2 실시예에서는 불확정 논리 회로(10)의 일 형태로서 플립플롭 회로가 사용되었다. 그러나, 전술된 바와 같이, 임의의 이들 플립플롭 회로에서 획득된 디지탈 신호 시퀀스는 "0"과 "1"의 출현 빈도에서 임의의 "불균일성"을 갖는다. 즉, "0"과 "1"간에 출현 빈도가 똑같지 않다. 등화 회로(20)는 "불균일성"을 보정하기 위한 디지탈 처리를 수행한다.

도 9는 본 실시예에 따른 등화 회로의 동작의 개념을 설명하기 위한 도면이다.

도 9에 도시된 바와 같이, 불확정 논리 회로(10)의 시간 순차 출력을 Qn, …, Qn+k 로서 입력하면, 이들 k+1개의 데이타에 대해 XOR(배타적 OR) 논리 연산이 수행된다. 그 결과를 T로 하면, 불확정 논리 회로(10)의 출력에서, T가 1이 되는 확률은 다음과 같다:

$$0.5 + 0.5\times(1-2p)^{k+1}$$

여기서, "1"의 출현 확률은 p이고, "0"의 출현 확률은 1-p이다. k가 증가할 때, 확률은 0.5에 근접하고, 불균일성이 보정된다.

제1 실시예에 따라 실제로 구성된 RS-FF에서, "불균일성"은 대략 p=0.1로 크다. k=10의 경우, T가 1이 되는 확률은 0.543이다. k=20의 경우에는 0.505이고, k=30인 경우에는 0.50이다. 즉, 확률이 0.5에 근접하게 되어 "불균일성"이 사라진다.

k의 값이 크면, 난수를 생성하는 속도는 감소한다. 그러나, 파워를 온과 오프 상태로 전환하는 주기가 30㎒ 라면, 디지탈 난수는 k=30 하에서도 1Mbit/sec 정도의 속도로 생성될 수 있다. 따라서, 대부분의 경우에 속도 문제는 실제로 문제시되지 않는다. Qn, …, Qn+ k 의 XOR, Qn+ 1, …, Qn+ (k+ 1) 의 XOR, Qn+ 2, …, Qn+ (k+ 2) 의 XOR 등과 같이 1씩 시프트하여 XOR 연산을 수행하면, 난수를 생성하는 속도가 감소하지 않는다.

이러한 방식으로 획득된 난수 시퀀스 데이타는 피드백 시프트 레지스터의 씨드로서 사용될 것이다.

또한, 하술된 방법을 사용함으로써, "0"과 "1"의 출현 빈도가 용이하게 동일하게 될 수 있다.

즉, 디지탈 신호 P가 "1"이 되는 확률이 p이고 디지탈 신호 Q가 "1"이 되는 확률이 q일 때, P와 Q의 XOR 연산값 T가 "1"이 되는 확률과 "0"이 되는 확률간의 차분은 다음과 같이 표현된다:

4(0.5-p)(0.5-q)

따라서, "1"이 되는 확률이 0.5라면, Q가 "1"이 되는 확률이 0.5가 아닌 경우에도 P와 Q의 XOR 연산값 T의 "0"의 출현 확률과 "1"의 출현 확률은 동일하게 된다.

플립플롭(10)에 대한 입력 신호가 분기되어 도 10에 도시된 바와 같이 T-형 플립플롭(20B)에 입력된다면, 주기가 2배가 되는 신호가 획득된다. 이 신호에서, "0"과 "1"이 동일 타이밍에서 플립플롭(10)의 출력으로 교대로 나타나게 된다. 당연히, 이 신호에서의 "0"과 "1"의 출현 비율은 동일하다. 따라서, 이 신호와 플립플롭(10)의 신호의 XOR 연산 출력 T에서, "0"과 "1"의 출현 확률은 동일하며, 그 출력이 무작위도가 높은 디지탈 난수 시퀀스로서 사용될 수 있다.

플립플롭(10)과 동일한 클록을 사용하는 도 11에 도시된 피드백 시프트 레지스터(FSR)(20C)에 의해 생성된 의사 난수 R은 "0"과 "1"을 동일하게 포함한다. 따라서, 이들 의사 난수 R과 플립플롭(10)의 출력의 XOR 연산값 T에서, "0"과 "1"의 출현 비율이 동일하여 무작위도가 높은 디지탈 난수 시퀀스로서 사용될 수 있다.

2개의 플립플롭을 사용하는 구성의 다른 특정 예가 도시되어 있다.

도 12는 이 특정 예를 도시하고 있는 개략도이다. 즉, T형 플립플롭으로부터의 주기가 2배가 된 출력과 D형 플립플롭에 의해 등화된 출력이 XOR 회로에 의해 연산된다.

이 경우에는 2개의 불안정 플립플롭(unstable flip-flop) 회로가 사용된다. 먼저, 기준 클록 신호가 2개로 분할되고, 이들 중의 하나가 T형 플립플롭을 통해 주기가 1/2로 변경된 후에 불확정 플립플롭 중의 하나에 공급된다. 그리고나서, 기준 클록의 1/2 주기를 갖는 불확정 랜덤 신호 A가 획득된다. 그러나, 이 신호 A에서는 "0"과 "1"의 출현 비율이 불균일하다.

분할된 기준 클록 신호의 나머지는 다른 불확정 플립플롭 회로에 공급되어 불확정 출력 Q와 반전된 출력 Q가 얻어진다. 반전된 Q가 D-형 플립플롭을 통해 1 기준 클록만큼 지연된 후에 A와 반전된 Q가 교대로 출력될 때, 이 신호는 "0"과 "1"이 각각 50%로 배열되는 랜덤 신호 B가 된다. 그러나, Q와 반전된 Q가 교대로 출현하기 때문에, 그 때에 일종의 규칙성이 존재한다. 이와 같이 획득된 랜덤 신호 B와 랜덤 신호 A의 XOR 연산에 의해, 전술된 2개의 예와 동일한 원리 때문에 0과 1이 균등하게 출현하는 난수가 획득될 수 있다.

(제4 실시예)

다음에는 불확정 논리 회로의 출력을 모니터링하고 이 출력을 본 발명의 제4 실시예의 출력으로 피드백하도록 구성된 난수 발생 회로를 설명한다.

도 13은 본 실시예에 따른 난수 발생 회로의 기본 부분의 구성을 도시하고 있는 개략도이다.

본 실시예에서, 등화 회로(20)는 도 7에서 설명된 불확정 플립플롭의 입력에 피드백된다. 이 피드백은 불확정 플립플롭의 "0"과 "1"의 출현 비율을 근사적으로 동등하게 한다.

더욱 구체적으로, 도 13에서, A측 트랜지스터 T7가 먼저 턴온될 때에 플립플롭의 출력이 "0"이 되는 것으로 가정한다. 도 13에 도시된 바와 같이, 설계 사양이 동일한 N-채널 MOS 트랜지스터 T7 및 T8이 피드백 회로(20E)와 전원 전압 입력 Vin 사이에 접속되고, B측 트랜지스터 T8의 게이트 전위가 사전에 접지 전위로 설정된다.

플립플롭의 출력은 디지탈 카운터(20D)에 의해 카운트되며, 카운트된 "0"과 "1"의 차분에 비례한 전위가 A측 MOS 트랜지스터 T7의 게이트에 인가된다. 출력에서 "1"이 더 빈번한 경우, A측 트랜지스터 T7의 게이트 전압이 플러스측으로 다소 시프트하여 채널 저항을 상당히 낮추고 A측으로의 전류 흐름을 수월하게 한다면, A측이 우선적으로 동작하고, 출력에서 "0"이 증가한다.

반대로, 출력에서 "0"이 더 빈번한 경우, A측 트랜지스터 T7의 게이트 전압이 마이너스측으로 시프트되어 채널 저항을 증가시킨다.

이러한 방식의 피드백은 플립플롭 출력에서 "0"과 "1"간의 출현 차이를 감소시키는 결과를 가져온다. 그러므로, 출력을 직접 난수로 사용하는 것도 가능하다.

또한, 제3 실시예로 설명된 바와 같이, "불균일성"을 제거할 수 있는 논리 회로가 결합되어 난수의 "불균일성"을 추가로 감소시킬 수도 있다. 이 경우, 전술된 XOR에 대한 데이타의 갯수 k가 더 적어질 것이며, 난수를 생성하는 속도가 향상될 수 있다.

(제5 실시예)

다음에는 불확정 논리 회로(10)의 플립플롭을 형성하는 NOR 회로(또는 NAND 회로)의 갯수를 증가시킴으로써 출력에서의 "0"과 "1"의 불균일성을 감소시키도록 구성된 본 발명의 제5 실시예를 설명한다.

반도체 회로가 대량 생산으로 제조되는 경우, 웨이퍼 상의 불균일 특성으로 인해 일부의 출력에서 극단적인 불균일성이 나타날 수도 있다. 예를 들어, 100%에 육박하는 "0"의 출현 빈도를 갖는 회로가 전체의 일부분에서 나타날 수도 있다. 출력의 극단적인 불균일성은 평활화 회로를 이용한 보정에 의해서도 난수의 품질 향상을 불가능하게 하며, 이러한 회로는 난수 발생 회로로서는 결함을 갖는다. 본 실시예는 이러한 결함 회로의 출현을 감소시키는데 적합하다.

도 14는 본 실시예의 구성에 대한 개념을 나타내고 있는 개략도이다. 본 실시예는 다수개(짝수개)의 플립플롭을 사용한다. 즉, 다수의(짝수개의) NOR 회로(또는 NAND 회로)가 도 14에 도시된 바와 같이 체인 접속으로 배열되어 각각의 NOR 회로의 출력이 다음 NOR 회로의 입력단 중의 하나에 공통된다면, 불확정 플립플롭과 동일한 동작이 실현된다.

즉, 입력이 "1"인 경우, 플립플롭의 모든 출력이 "0"이 될 때에 회로는 안정한 상태가 된다. 즉, 입력 "1"이 리셋(R) 신호로 간주될 수 있다. 입력이 "0"로 변경되면, NOR 회로는 인버터에 상당하게 되고, "1"과 "0"이 교대로 나타날 때에 안정한 상태가 된다. 즉, 입력 "0"이 세트(S) 신호로 간주될 수 있다. NOR 회로로부터의 출력이 "0", "1", "0", "1"의 시퀀스로 나타나는지 아니면 "1", "0", "1", "0"의 시퀀스로 나타나는지의 여부는 유지된 w 상태에 좌우된다. 그러나, 이전 상태(입력으로 "1"이 인가되는 상황에 응답하는 상태)가 "0", "0", "0", "0"이기 때문에, "0"과 "1"의 어느 시퀀스가 실제로 출현할지는 불확정이다.

이 경우, 다수의 NOR 회로가 공존하기 때문에, 2개의 NOR 회로로 플립플롭이 구성되는 구성보다는 출력의 불균일성이 더 작다. 당연히, NOR 회로가 증가할 때 출력의 불균일성은 더 작아진다.

이 특정 예의 경우, 홀수 번호의 NOR 회로의 출력은 원칙적으로 그 값이 서로 동일하고, 짝수 번호의 NOR 회로의 출력 또한 원칙적으로 그 값이 서로 동일하다. 홀수 번호 출력 또는 짝수 번호 출력은 전술된 등화 회로로 결합되어 더 높은 품질의 난수가 얻어진다.

다음에는 발진기 회로로부터의 신호를 짝수개의 플립플롭에 제공하도록 구성된 본 실시예의 제2 특정 예를 설명한다.

도 15a 및 도 15b는 이 특정 예의 기본 부분의 구성을 도시하고 있는 개략도이다. 도 15a에 도시된 바와 같이, 많은 짝수개의 NOR 회로(또는 NAND 회로)가 불확정 플립플롭을 형성하도록 구성되고, 각각의 NOR 회로에는 독립 입력이 사용된다. 그리고나서, 각각의 NOR 회로에 "0" 또는 "1" 및 "0"이 교대로 제공된다. 이에 의해 무작위도를 위한 요소가 증가되어 높은 품질의 난수를 작성하는데 기여한다.

이 원리는 도 15a 및 도 15b에 도시된 바와 같이 4개의 NOR 회로를 사용하는 구성을 가지고 이하에 설명된다. 각각의 NOR 회로에 대한 입력과 출력의 조합을 편의를 위해 [X1, X2, X3, X4 : Q1, Q2, Q3, Q4]로 표현하면, 이들은 예를 들어 다음과 같이 된다:

[1, 0, 0, 0 : 0, 1, 0, 1]

[1, 1, 0, 0 : 0, 0, 1, 0]

[1, 0, 1, 0 : 0, 1, 0, 1]

[1, 0, 0, 1 : 0, 1, 0, 0]

[1, 1, 1, 0 : 0, 0, 0, 1]

출력 Q1 내지 Q4에서 "0"과 "1"이 교대로 배열하지 않는 경우, 모든 입력 X로서 "0"이 입력된다면, 모든 NOR 회로는 인버터에 상당하게 된다. 따라서, X와 Q는 다음과 같이 된다:

[0, 0, 0, 0 : 0, 1, 0, 1] 또는

[0, 0, 0, 0 : 1, 0, 1, 0]

이 경우, 어느 시퀀스가 실제로 출현할지는 불확정이다. 입력 X가 무작위도(randomness)를 갖는다면, 불확정 플립플롭의 무작위도와 입력 X의 무작위도와의 상호작용 효과는 난수의 품질을 향상시킨다. 랜덤한 입력을 위한 방법으로서는 도 16에 도시된 바와 같이 주파수가 상이한 비동기식 발진기 회로를 사용하는 것이 효과적이다.

보다 구체적으로 설명하면, 비동기식 발진기 회로와 D-형 래치(latch)가 각각의 NOR 회로와 관련하여 제공된다. 비동기식 발진기 회로는 그들의 출력단에 버퍼를 포함하여 그들의 출력이 "0" 또는 "1"로 변환되도록 하는 것이 바람직하다. 그러나, 발진기 회로의 출력이 멀티바이브레이터와 같이 디지탈화된다면, 버퍼를 포함할 필요가 없다. 비동기식 발진기 회로로부터의 출력은 표준 클록과 동기하여 래치되고, 래치된 신호와 클록을 AND 연산함으로써, "0" 또는 "1"과 "0"이 교대로 나타나는 신호가 획득된다. 이러한 신호가 입력 X로 사용된다면, 플립플롭은 도 15b에 도시된 바와 같이 특정값으로서의 "0"과 불확정값으로서의 "0" 또는 "1"을 교대로 출력한다. 그러므로, 불확정값을 추출함으로써, 디지탈 난수가 획득될 수 있다.

여기서 적당한 특정 출력을 갖는 논리 회로로 독립 입력 X1 내지 X4를 처리하는 것만으로는 난수가 작성될 수 없다는 점에 유의하기 바란다. 각각의 입력 X가 비동기이기는 하지만, 이들 입력은 주기성을 나타낸다. 따라서, 이들 출력을 논리 회로에서 단순히 조합하는 것에 의해서는 출력에 항상 주기성이 나타나고, 일반적으로 고품질 난수가 획득되지 않는다. 고품질 난수는 불확정 플립플롭을 통해서만 획득된다.

이와 달리, 도 17에 도시된 바와 같이, 의사 난수를 발생할 수 있는 LFSR(선형 피드백 시프트 레지스터)을 사용하여 시프트 레지스터 SR 중의 하나로부터 랜덤하게 입력하는 것이 편리하고 효과적이다. 도 17에서는 도 16과 달리 NAND 회로가 2단으로 접속되어 있다. 이들의 논리 연산은 2단으로 접속된 AND 회로와 NOR 회로의 논리 연산과 동일하다.

원칙적으로, 홀수 번호 출력은 그 값이 서로 동일하고, 짝수 번호 출력도 그 값이 서로 동일하다. 각각의 짝수 번호 출력과 홀수 번호 출력은 전술된 등화 회로로 조합되어 품질이 더 높은 난수가 획득된다.

(제6 실시예)

다음에는 제5 실시예와 상이한 방식으로 불확정 논리 회로(10)의 플립플롭을 형성하는 NOR 회로(또는 NAND 회로)를 증가시킴으로써 "0"과 "1"의 출현 빈도간의 불균일성을 감소시키는 본 발명의 제6 실시예를 설명한다.

도 18a 및 도 18b는 본 실시예에 따른 회로의 기본 부분을 도시하고 있는 개략도이다. 도 18a는 5개의 UFF(Unsettlable Flip-Flop)를 사용하여 회로를 구성하는 특정 예를 도시하고 있다. 도 18b에 도시된 바와 같이, 각각의 UFF는 2개의 NOR 회로로 구성된 불확정 플립플롭이 될 수도 있다.

UFF의 경우에는 "0"과 "1"의 출현 빈도가 입력 펄스의 전압 레벨에 좌우되곤 한다. 즉, 입력 펄스가 디지탈 회로의 기준 전압인 공급 전압 VDD 이하로 강하되면, UFF는 출력에서 더 높거나 더 낮은 "1"의 출현 빈도를 나타내곤 한다. 이것은 UFF를 형성하는 NOR 회로가 약간이기는 하지만 임계 전압이 변화하기 때문이다. 도 19는 UFF에 입력된 펄스 전압에 대한 "1"의 출현 확률의 의존도를 예시하는 그래프이다. 즉, 도 19에는 입력 펄스의 주기가 2㎲이고 펄스폭이 65㎱이고 펄스 전압 Vrs가 변경될 때에 UFF 출력에서의 "1"의 발생 확률이 도시되어 있다. 도 19에서는 2 볼트의 소스 전압 VDD에 접속된 UFF 가 이용된다.

도 19로부터 펄스 전압 Vrs이 상승할 때에 "1"의 출현 확률이 연속적으로 증가하다는 것을 알 수 있을 것이다. 펄스 전압 Vrs이 1.3 볼트에 근접하게 도달할 때, "1"의 출현 확률은 대략 0.5가 된다. 즉, 이 레벨의 펄스 전압이 UFF 출력에서의 "0"과 "1"의 출현 확률을 실질적으로 동일하게 한다.

따라서, 도 18a에 도시된 바와 같이, 전압이 상이한 펄스를 복수의 UFF에 제공함으로써, "0"과 "1"의 출현 빈도간의 작은 차이를 갖는 출력이 이들 UFF의 하나 또는 그 이상으로부터 획득될 수 있다.

도 18a에서, 5개의 UFF에 대한 입력은 VDD에서 VDD의 20%까지 순차적으로 강하된다. 5개의 UFF의 출력의 XOR 연산이 행해질 때, XOR 출력에서의 "0"과 "1"의 출현 빈도간의 차이는 이들 5개의 UFF의 "0"과 "1"의 출현 빈도의 차이의 최저치와 같거나 작다. 이 원리는 도 9에 도시된 등화 회로(20A)의 XOR 기능으로서 이미 설명된 것과 동일하다.

도 18a가 5개의 UFF를 사용하는 구성을 도시하고 있지만, UFF의 갯수가 증가하고 그들의 소스 전압이 더욱 미묘하게 변화할 때, 출력에서의 "0"과 "1"의 출현 빈도의 불균일성을 감소시키는 효과가 향상된다.

지금까지, 본 발명의 실시예들을 특정 예와 관련하여 설명하였다. 그러나, 본 발명은 이러한 특정 예로 제한되지는 않는다.

예를 들어, 본 발명의 실시예에 사용된 불확정 논리 회로와 등화 회로의 구체적인 구성은 이들 특정 예로 제한되지 않고, 본 발명은 이러한 기능과 동작을 위한 어떠한 회로를 사용하는 어떠한 변형도 본 발명의 기술사상에 포함되는 것으로 한다.

예를 들어, 병렬 또는 직렬로 연결된 출력이 불확정인 복수의 플립플롭을 포함하는 논리 회로의 출력이 "0"과 "1"의 출현 빈도를 동일하게 하기 위한 논리 회로에 제공되도록 난수 발생 회로를 구성하는 것도 효과적이며, 이것 또한 본 발명의 기술 범위에 포함되는 것이다.

또한, 전술된 실시예 중에서, 출력이 불확정인 디지탈 회로와 디지탈 출력에서의 빈도를 보정하기 위한 회로를 부분적으로 결합한 것도 난수 발생 회로로서 사용 가능하며, 이들도 본 발명의 기술 범위에 포함된다.

발명의 효과

본 발명의 임의의 실시예에 따른 난수 발생 회로에 의해 작성된 디지탈 난수는 난수로 직접 사용되거나 새로운 난수를 작성하기 위해 피드백 시프트 레지스터의 씨드로서 사용될 수 있다.

전술된 바와 같이, 본 발명의 실시예에 따르면, 예를 들어 플립플롭형 논리 회로를 사용함으로써 더 적은 수의 논리 게이트로 난수 발생 회로를 구성할 수 있어 회로의 크기를 축소할 수 있다.

동시에, "0"과 "1"의 출현 빈도를 보정하기 위한 등화 회로를 상당히 작은 크기의 논리 회로로 구성할 수 있다.

난수의 공급원이 되는 현상이 불확정 논리 회로를 형성하는 구성요소의 물리적인 현상에 기초를 두고 있기 때문에, 단일 입력값에 응답하여 불확정 출력이 획득된다. 따라서, 난수 시퀀스는 어떠한 주기성도 나타내지 않으며, 난수가 추정될 수 있는 의사 난수와는 다른 고품질 난수를 획득할 수 있다.

더욱이, 불확정 논리 회로의 출력과 동일한 타이밍에서 반복적으로 배열된 "0"과 "1"을 포함하는 신호가 일정 주기의 클록 신호를 분기함으로써 T-형 플립플롭을 통해 발생되어, 이 신호와 불확정 논리 회로의 출력 신호의 배타적 OR가 연산될 때, 연산 출력 T는 "0"과 "1"의 동일한 출현 확률과 높은 무작위도를 갖는 디지탈 난수 시퀀스로서 사용될 수 있다.

즉, 본 발명은 소형이면서 저렴한 회로를 사용하여 무작위도가 높은 난수를 실현하고 이에 의해 예를 들어 IC 카드에 응용이 가능하여 보안을 신뢰할 수 있는 상업적인 카드 시스템을 실현할 수 있다는 점에서 커다란 산업상의 장점을 갖는다.

본 발명의 이해를 보다 용이하게 하기 위해 실시예의 형태로 본 발명을 설명하였지만, 본 발명은 발명의 기술사상에서 일탈함이 없이 여러 방식으로 구체화될 수 있다는 점에 유의해야 한다. 따라서, 본 발명은 첨부된 청구범위에 한정된 바와 같은 본 발명의 원리로부터 벗어나지 않은채 구현될 수 있는 모든 가능한 실시예와 도시된 실시예의 변형예를 포함하는 것으로 이해되어야 한다.

(57) 청구의 범위

청구항 1.

디지털 입력값에 대하여 일의적으로 결정되지 않는 디지털 출력값을 제공하는 플립플롭형의 논리 회로를 포함하는 불확정 논리 회로와,

상기 불확정 논리 회로로부터 출력되는 상기 디지털 출력값에 있어서의 「0」과「1」의 출현 빈도를 균등하게 하기 위한 등화 회로

를 포함하고,

상기 불확정 논리 회로는, 4개 이상의 짝수의 NOR 회로 또는 NAND 회로를 포함하고, 이들 NOR 회로 또는 NAND 회로는, 각각의 회로의 출력 단자가 그 다음 회로의 입력 단자의 한쪽에 연쇄적으로 접속되어 이루어지는 것을 특징으로 하는 난수 발생 회로.

청구항 2.

제1항에 있어서,

상기 불확정 논리 회로는, 상기 4개 이상의 짝수의 NOR 회로 또는 NAND 회로의 각각의 입력 단자의 다른 쪽을 공통 접속하여 「1」을 입력한 후에 「O」을 입력함으로써 상기 일의적으로 결정되지 않는 디지털 출력값을 제공하는 것을 특징으로 하는 난수 발생 회로.

청구항 3.

제1항에 있어서,

상기 불확정 논리 회로는, 상기 4개 이상의 짝수의 NOR 회로 또는 NAND 회로의 각각의 입력 단자의 다른 쪽에 독립적으로 「0」 및「1」 중 어느 하나와, 「0」을 교대로 입력함으로써 상기 일의적으로 결정되지 않는 디지털 출력값을 제공하는 것을 특징으로 하는 난수 발생 회로.

청구항 4.

제3항에 있어서,

상기「0」 및 「1」중 어느 하나는, 상기 4개 이상의 짝수의 NOR 회로 또는 NAND 회로의 각각에 대응시켜 설치된, 비동기이고 주파수가 상호 다른 발진 회로에 의해 형성되는 것을 특징으로 하는 난수 발생 회로.

청구항 5.

디지털 입력값에 대하여 일의적으로 결정되지 않는 디지털 출력값을 제공하는 플립플롭형의 논리 회로를 포함하는 불확정 논리 회로와,

상기 불확정 논리 회로로부터 출력되는 상기 디지털 출력값에 있어서의 「0」과「1」의 출현 빈도를 균등하게 하기 위한 등화 회로

를 포함하고,

상기 불확정 논리 회로는, 복수의 RS형의 플립플롭을 포함하고, 이들 플립플롭마다 크기가 다른 펄스 전압을 입력하고, 이들 플립플롭으로부터의 출력의 배타적 논리합을 출력으로 하는 것을 특징으로 하는 난수 발생 회로.

청구항 6.

제5항에 있어서,

상기 크기가 다른 펄스 전압 중 적어도 어느 하나는, 디지털 회로의 기준이 되는 전원 전압보다도 절대값이 작은 것을 특징으로 하는 난수 발생 회로.

청구항 7.

제1항 내지 제6항 중 어느 한 항에 있어서,

상기 등화 회로는,

상기 플립플롭형의 논리 회로로부터 출력되는 「0」과「1」의 출현 빈도를 카운트하는 카운트 회로와,

상기 카운트 회로에 의해 카운트한 상기 출현 빈도에 기초한 피드백 신호를 상기 플립플롭형의 논리 회로에 제공하는 피드백 회로

를 포함하는 것을 특징으로 하는 난수 발생 회로.

청구항 8.

제1항 내지 제6항 중 어느 한 항에 있어서,

상기 등화 회로는, 상기 불확정 논리 회로로부터 출력된 복수의 디지털 신호의 배타적 논리합을 연산하여, 난수로서 출력하는 것을 특징으로 하는 난수 발생 회로.

청구항 9.

제1항 내지 제6항 중 어느 한 항에 있어서,

상기 등화 회로는, 「0」과 「1」의 출현 빈도가 1:1인 디지털 신호 열과, 상기 불확정 논리 회로로부터 출력되는 디지털 신호 열과의 배타적 논리합을 연산하여, 디지털 난수 열로서 출력하는 것을 특징으로 하는 난수 발생 회로.

청구항 10.
삭제

청구항 11.
삭제

청구항 12.
삭제

청구항 13.
삭제

청구항 14.
삭제

청구항 15.
삭제

청구항 16.
삭제

청구항 17.
삭제

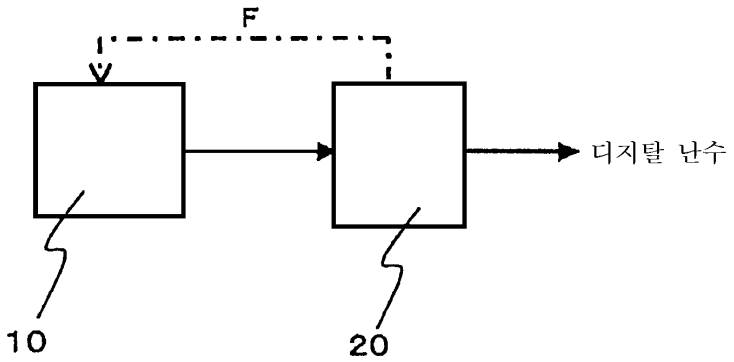
청구항 18.
삭제

청구항 19.
삭제

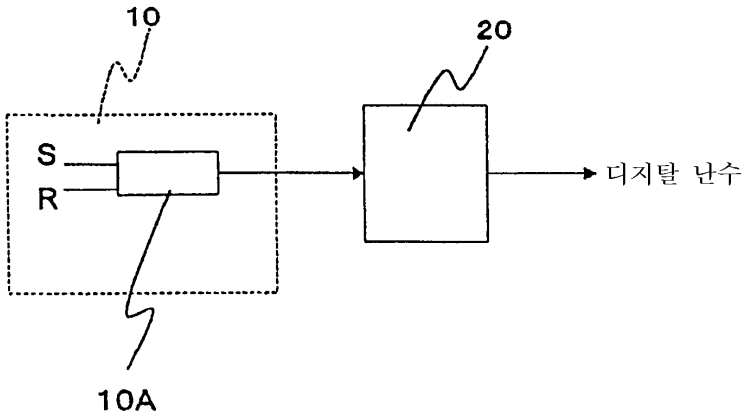
청구항 20.
삭제

도면

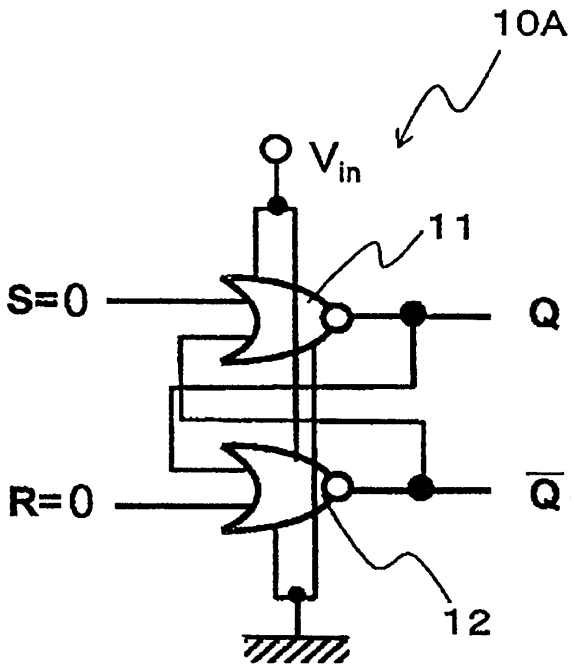
도면1



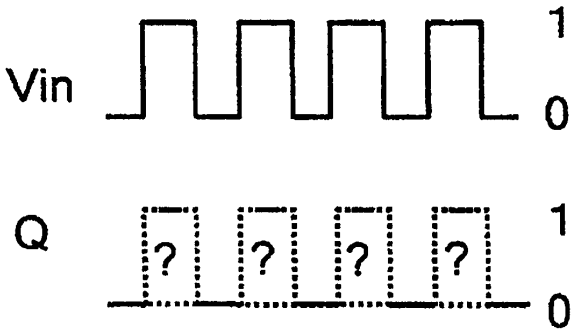
도면2



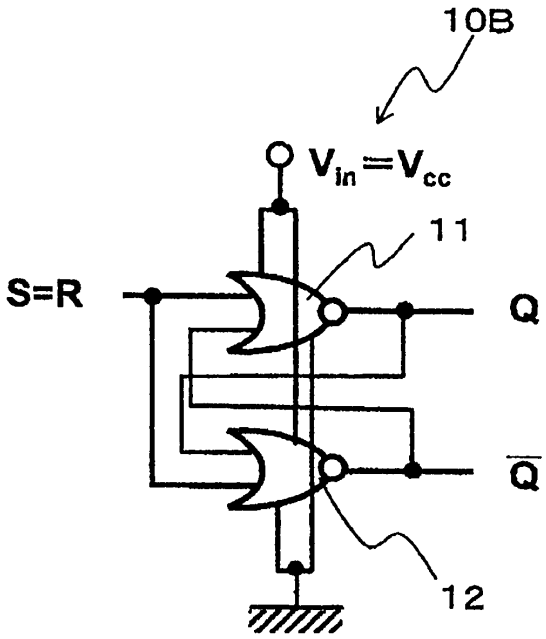
도면3



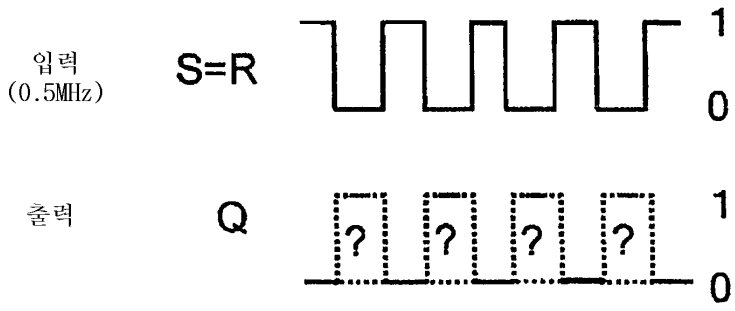
도면4



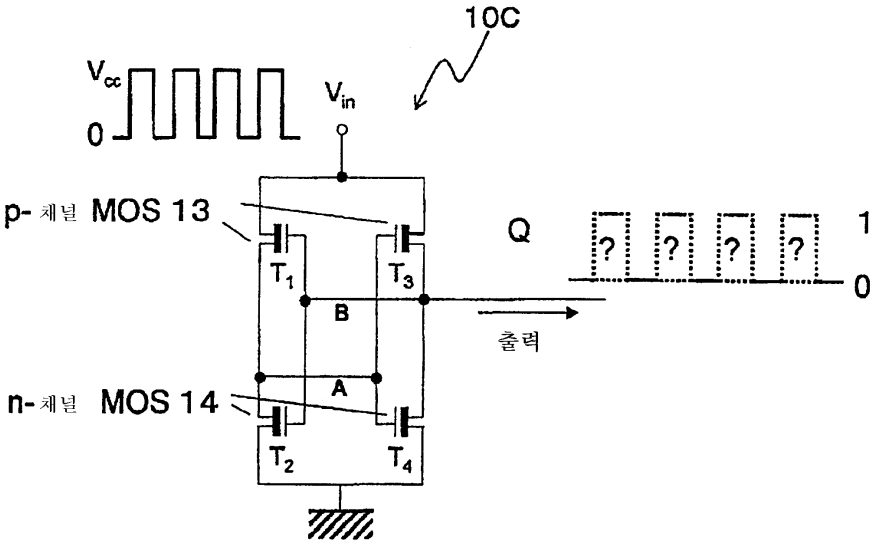
도면5



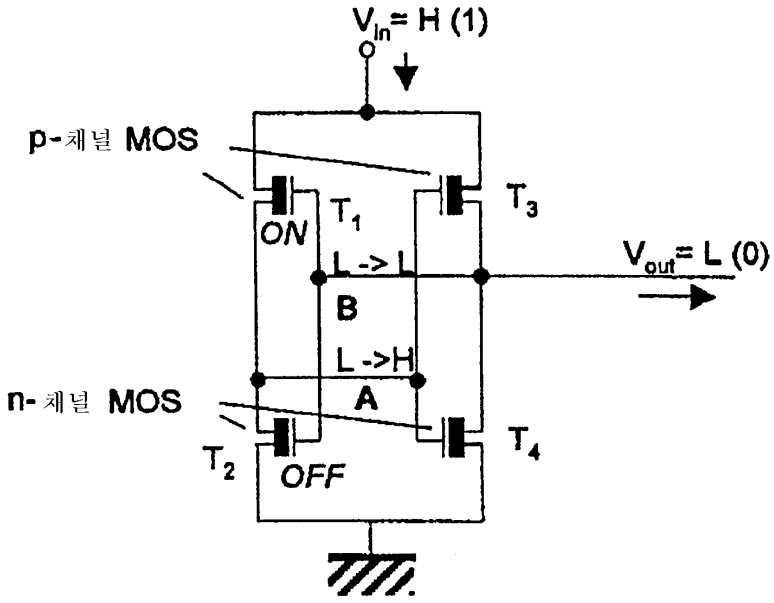
도면6



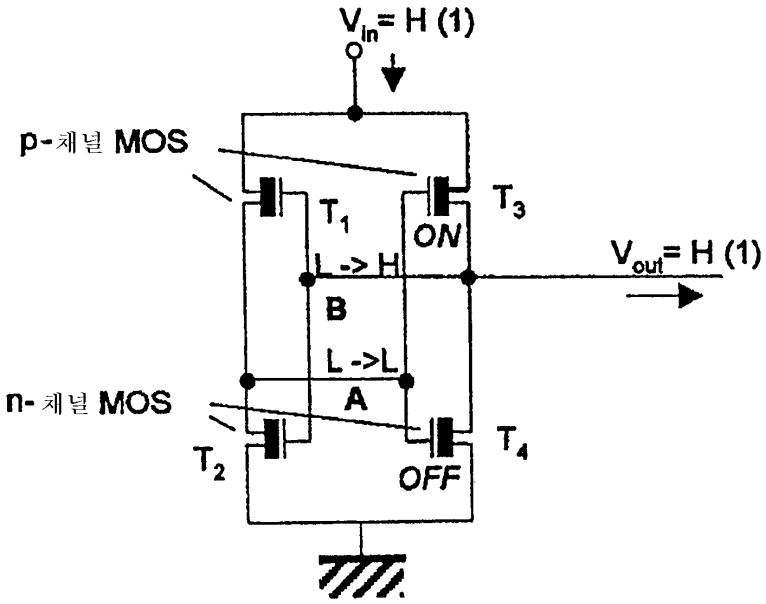
도면7


10C
V_{in}
p-채널 MOS 13
T_1
T_3
B
Q
1
0
출력
A
n-채널 MOS 14
T_2
T_4

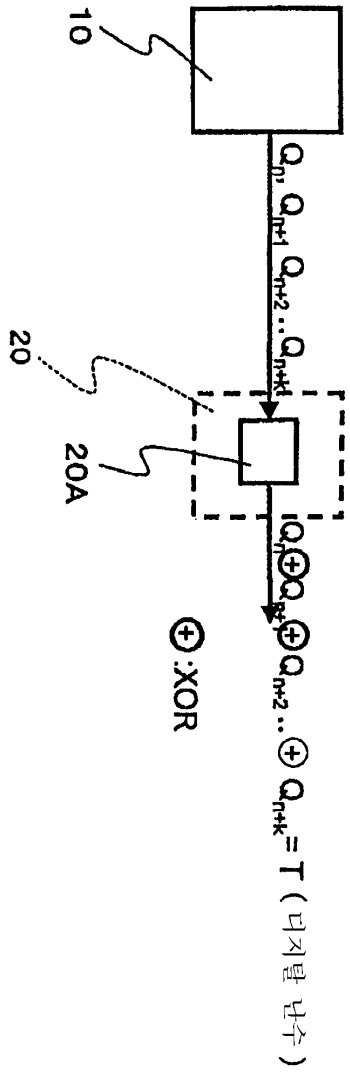
도면8a


V_{In}= H (1)
p-채널 MOS
T_1
T_3
ON
L -> L
V_{out}= L (0)
B
L ->H
A
n-채널 MOS
T_2
T_4
OFF

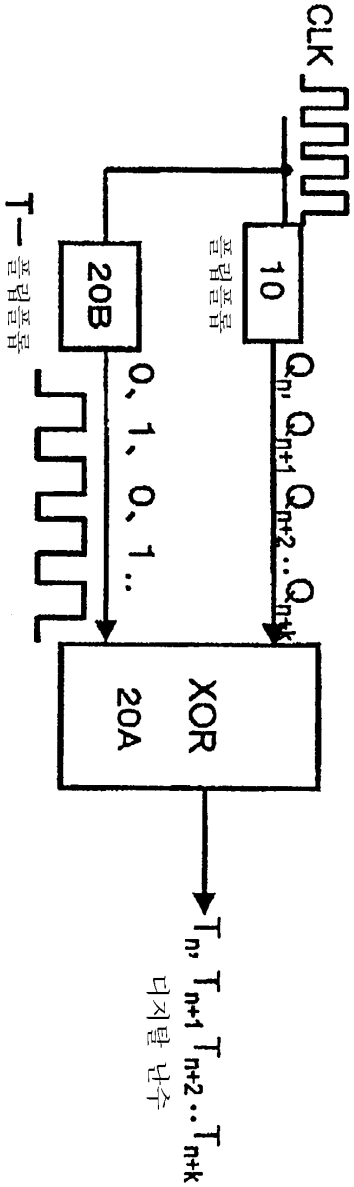
도면8b



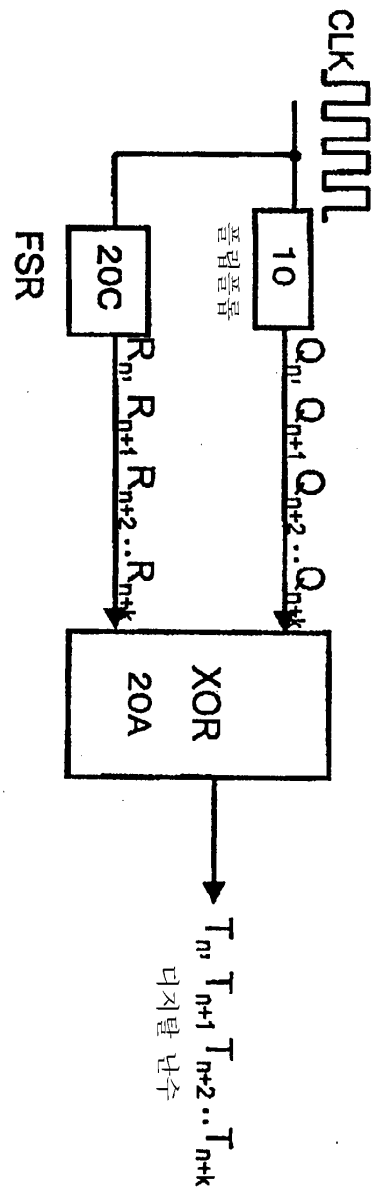
도면9



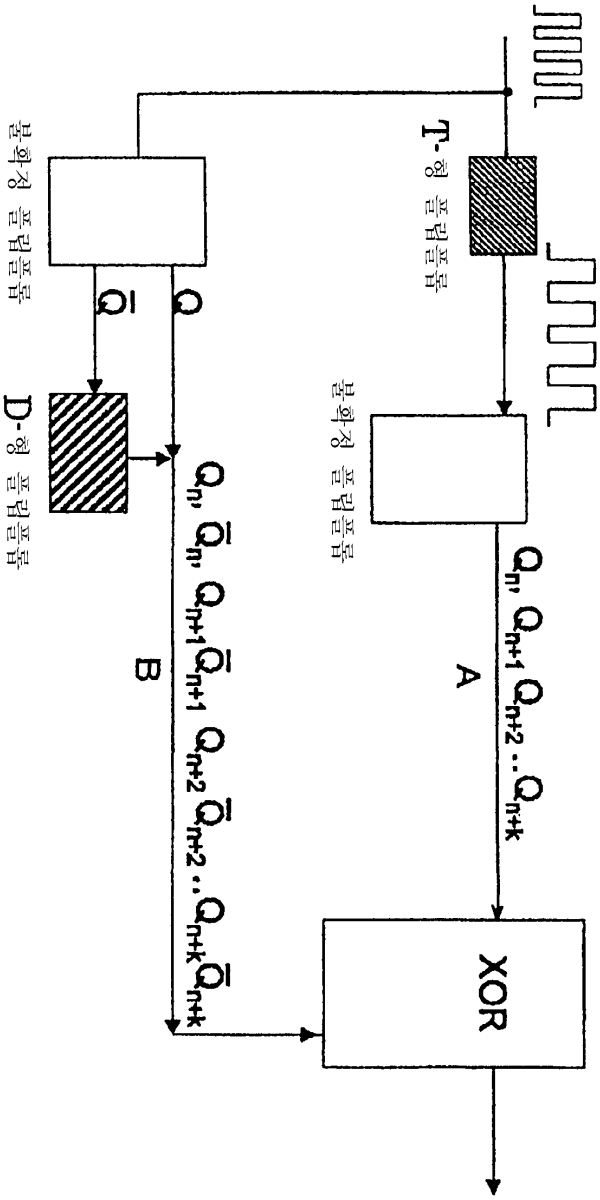
도면10


CLK
10
플립플롭
20B
T- 플립플롭
0, 1, 0, 1..
$Q_n, Q_{n+1} Q_{n+2}..Q_{n+k}$
XOR
20A
$T_n, T_{n+1} T_{n+2}..T_{n+k}$
디지탈 난수

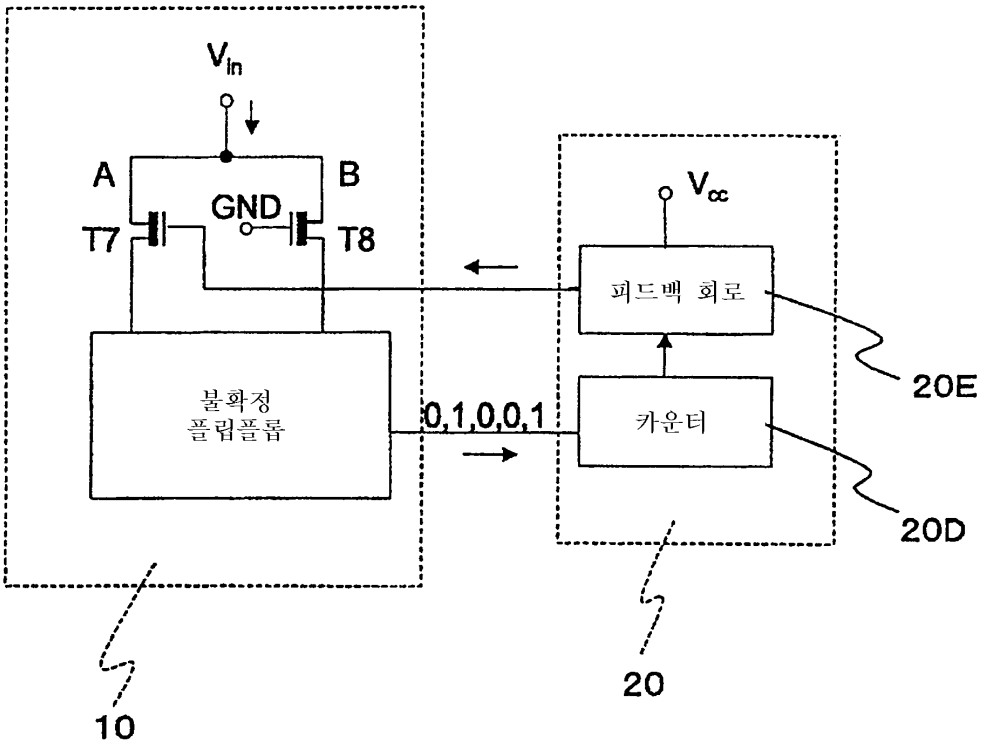
도면11


CLK
10
플립플롭
20C
FSR
Q_n, Q_{n+1} Q_{n+2}..Q_{n+k}
R_n, R_{n+1} R_{n+2}..R_{n+k}
XOR
20A
T_n, T_{n+1} T_{n+2}..T_{n+k}
디지탈 난수

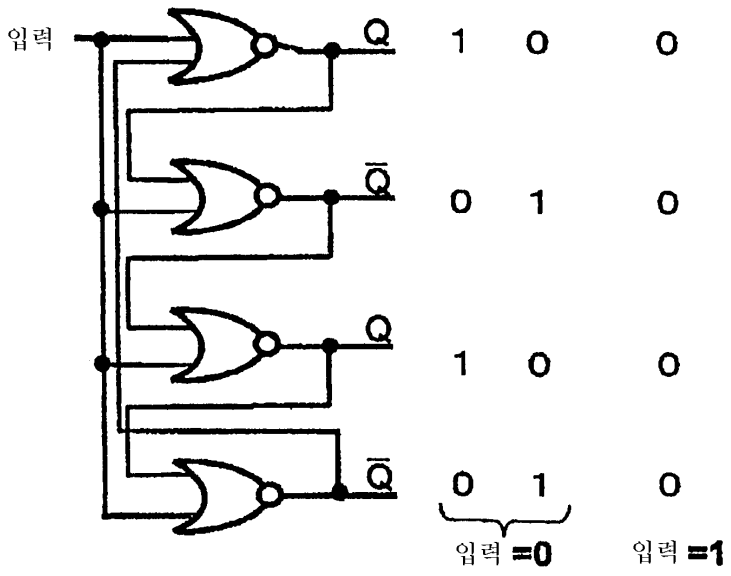
도면12


T-형 플립플롭
불확정 플립플롭
D-형 플립플롭
불확정 플립플롭
Q
Q̄
A
B
XOR
Qn, Qn+1 Qn+2 .. Qn+k
Qn, Q̄n, Qn+1 Q̄n+1 Qn+2 Q̄n+2 .. Qn+k Q̄n+k

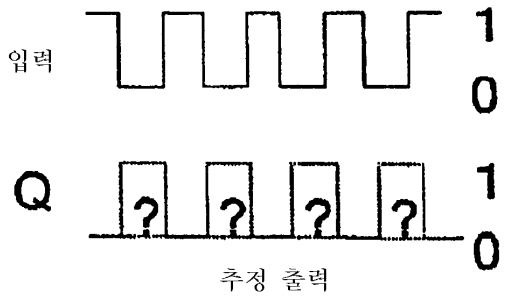
도면13


V_{In}
A
B
GND
T7
T8
불확정
플립플롭
0,1,0,0,1
V_{cc}
피드백 회로
카운터
20E
20D
10
20

도면14a

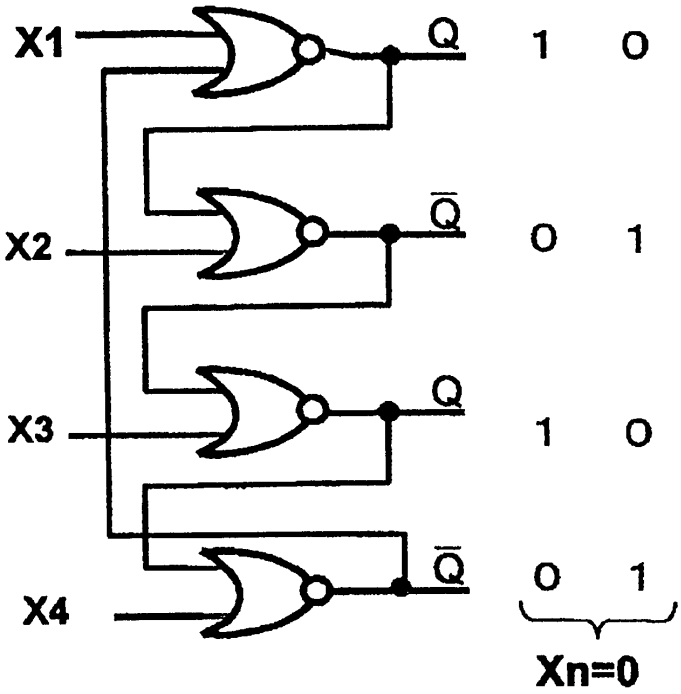

입력
Q
$\bar{Q}$
Q
$\bar{Q}$
1 0 0
0 1 0
1 0 0
0 1 0
입력 =0
입력 =1

도면14b



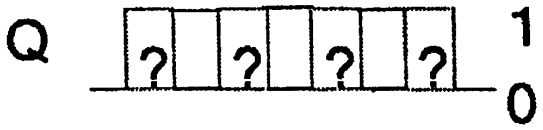
추정 출력

도면15a

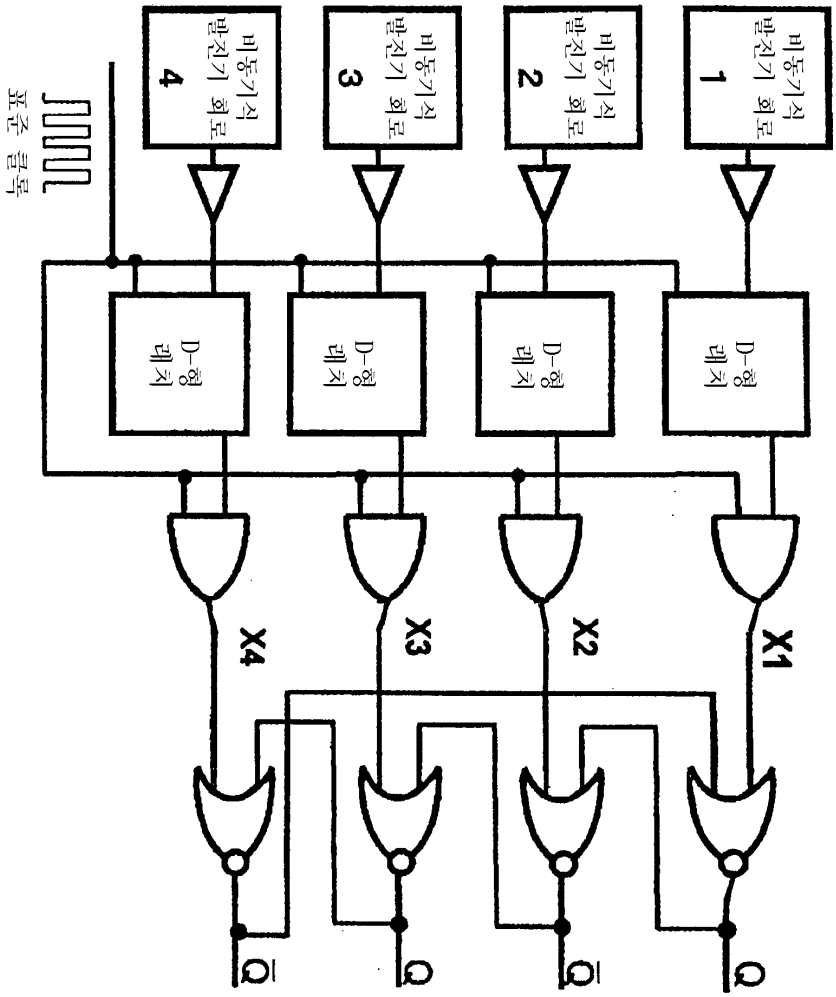


도면15b

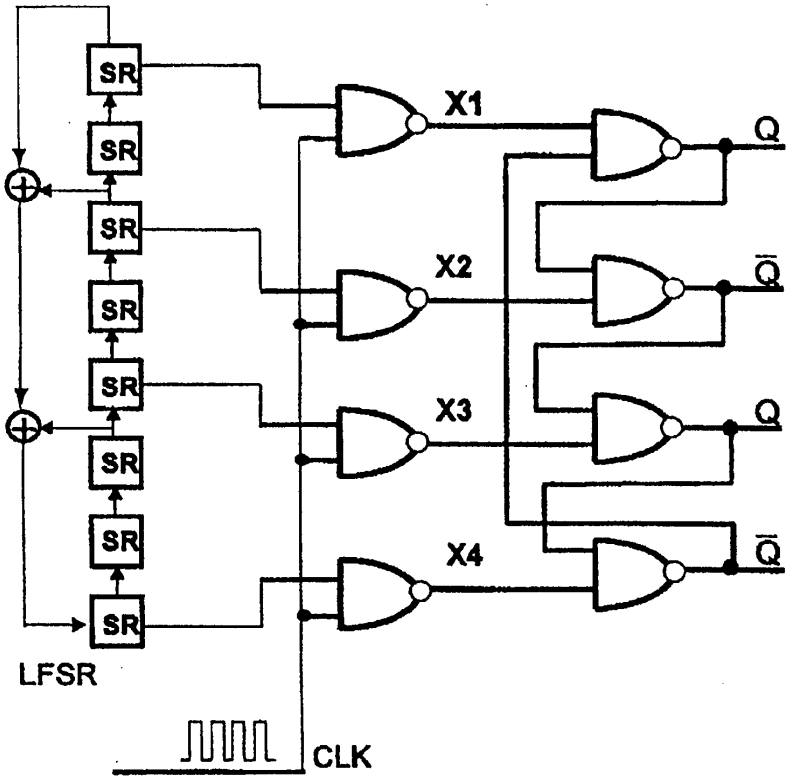
추정 출력



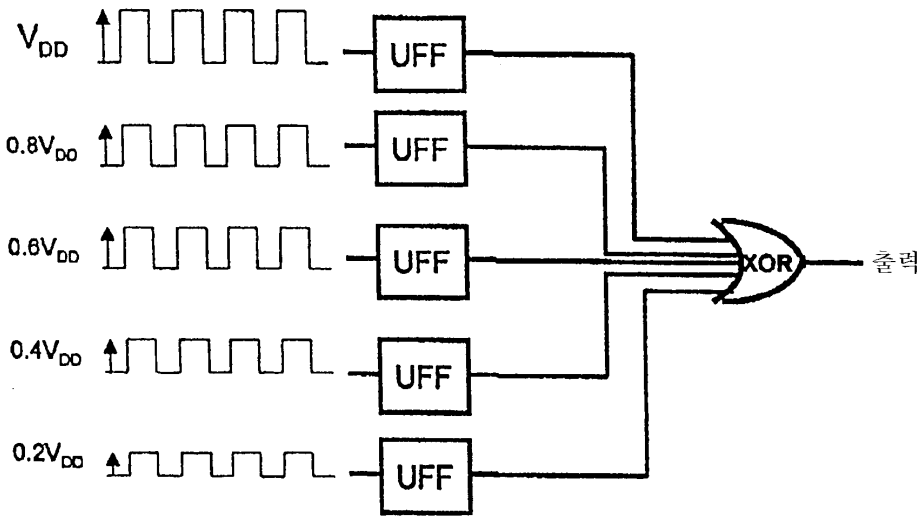
도면16


비동기식 발진기 회로 1
비동기식 발진기 회로 2
비동기식 발진기 회로 3
비동기식 발진기 회로 4
표준 클록
D-형 래치
D-형 래치
D-형 래치
D-형 래치
X1
X2
X3
X4
Q
Q
Q
Q

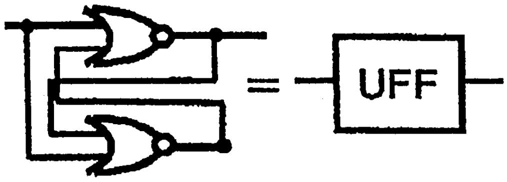
도면17


SR
SR
SR
SR
SR
SR
SR
SR
LFSR
X1
X2
X3
X4
Q
$\bar{Q}$
Q
$\bar{Q}$
CLK

도면18a


V_{DD}
$0.8V_{DD}$
$0.6V_{DD}$
$0.4V_{DD}$
$0.2V_{DD}$
UFF
UFF
UFF
UFF
UFF
XOR
출력

도면18b



도면19