(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2014 년 1 월 9 일 (09.01.2014)

WIPO | PCT

(10) 국제공개번호
WO 2014/007583 A1

(51) 국제특허분류:
G06F 7/58 (2006.01) *H03K 19/173* (2006.01)

(21) 국제출원번호: PCT/KR2013/006008

(22) 국제출원일: 2013 년 7 월 5 일 (05.07.2013)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2012-0073464 2012 년 7 월 5 일 (05.07.2012) KR

(71) 출원인: **부산대학교 산학협력단 (PUSAN NATIONAL UNIVERSITY INDUSTRY--UNIVERSITY COOPERATION FOUNDATION)** [KR/KR]; 609-735 부산시 금정구 부산대학로 63 번길 2 (장전동, 부산대학교), Busan (KR).

(72) 발명자: **김호원 (KIM, Howon)**; 604-051 부산시 사하구 다대 1 동 1627 번지 롯데캐슬몰운대아파트 218-1603, Busan (KR). **이동건 (LEE, Donggun)**; 611-772 부산시 연제구 거제 1 동 월드메르디앙아파트 103-1402, Busan (KR).

(74) 대리인: **오위환 (OH, Wihwan)**; 135-080 서울시 강남구 역삼동 601-18 은성빌딩 5 층, Seoul (KR).

(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

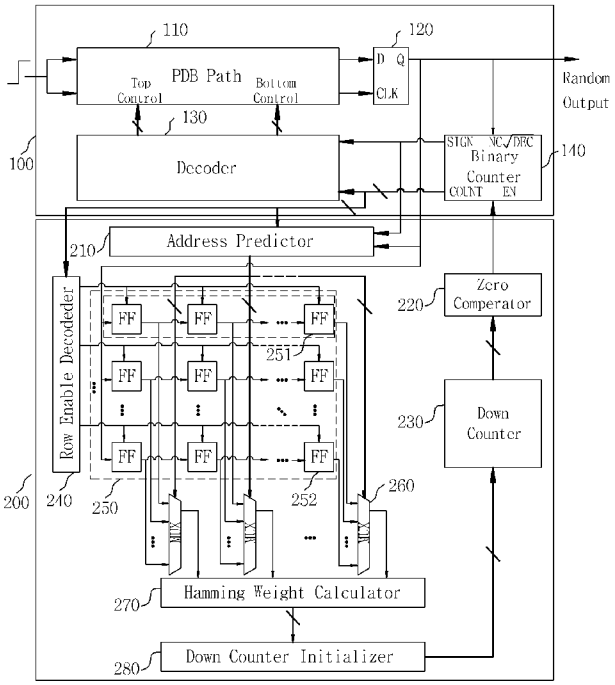
공개:

— 국제조사보고서와 함께 (조약 제 21 조(3))

[다음 쪽 계속]

(54) Title: APPARATUS AND METHOD FOR ENHANCING PERFORMANCE OF FPGA-BASED TRUE RANDOM NUMBER GENERATOR

(54) 발명의 명칭 : F P G A 기반된 진정한 난수 생성기의 성능 향상을 위한 장치 및 방법



(57) Abstract: The objective of the present invention is to provide an apparatus and a method for improving randomness when generating a random bit sequence by using a field-programmable gate array (FPGA), and enhancing the performance of an FPGA-based true random number generator (TRNG) so as to increase throughput. In existing methods for generating the TRNG by controlling a PDB and a PI, a filtering technique is used to remove output which is generated when not metastable, whereas the present invention applies a technique which minimizes the state in which a non-metastable value is outputted. To this end, the present invention distributes a large quantity of time slots in a metastable output state on the basis of previous output records that are saved, and a memory form similar to cash is used for efficiently saving output records.

(57) 요약서: 본 발명은 FPGA(Field-Programmable Gate Array)를 이용하여 랜덤한 비트 시퀀스를 생성할 때, 랜덤 특성을 향상시키고, 처리량(throughput)을 늘리기 위한 FPGA 기반된 진정한 난수 생성 장치의 성능 향상을 위한 장치 및 방법을 제공하기 위한 것으로서, PDB 와 PI 제어를 통한 TRNG 의 구현에 있어서, 종래의 구현에서 Metastable 하지 못한 경우에 발생하는 출력을 제거하기 위해 필터링 기법을 사용하는 것에 반해 Metastable 하지 못한 값이 출력되는 상태를 최소화 하는 기법을 적용하였으며, 이를 위해 이전의 출력 기록을 저장하여 이를 바탕으로 Metastable 한 출력 상태에 많은 Time Slot 을 배분하도록 하였고, 효율적으로 출력 기록을 저장하기 위해 캐쉬와 유사한 형태의 메모리 형태를 사용하였다.

WO 2014/007583 A1

— 청구범위 보정 기한 만료 전의 공개이며, 보정서를 접수하는 경우 그에 관하여 별도 공개함 (규칙 48.2(h))

명세서

발명의 명칭: F P G A 기반된 진정한 난수 생성기의 성능 향상을 위한 장치 및 방법

기술분야

[1] 본 발명은 난수 생성기에 관한 것으로, 특히 FPGA(Field-Programmable Gate Array)를 이용하여 랜덤한 비트 시퀀스를 생성할 때, 랜덤 특성을 향상시키고, 처리량(throughput)을 늘리기 위한 FPGA 기반된 진정한 난수 생성 장치의 성능 향상을 위한 장치 및 방법에 관한 것이다.

배경기술

[2] 랜덤 숫자는 암호화에 있어 필수적인 요소로서, 비밀 값을 생성하거나 PKI(Public Key Infrastructure)에 있어 공개키를 생성하거나, 디지털 서명을 작성할 때, 혹은 인증 프로토콜 등에서 사용되고 있다. 이때, 랜덤을 생성하는 방법에는 랜덤 숫자와 유사한 형태의 의사난수(pseudorandom) 숫자를 생성하는 방법과, 예측 불가능하며 재현 불가능한 진정한 랜덤 값을 생성하는 진정한 난수(true randon number)를 생성하는 방법이 존재한다.

[3] 상기 의사난수는 암호화가 아닌 일반 응용 프로그램에서는 랜덤 숫자와 유사한 형태로 사용하기에 부족함이 없지만, 암호화에서 사용될 대는 주의가 필요하다. 즉, 의사난수는 어디까지나 랜덤 숫자와 비슷한 형태의 수자일 뿐이며, 예측 가능하며 재현 가능하기 때문에 암호화에 사용될 경우 심각한 취약점이 될 수 있다. 따라서 랜덤 숫자가 암호화에 사용되기 위해서는 반드시 진정한 난수 생성기(True Random Number Generator : TRNG)로부터 생성될 필요가 있다.

[4] 상기 진정한 난수 생성기(TRNG)는 FPGA(Field-Programmable Gate Array)를 이용해서도 구현되기도 하는데, FPGA는 빠른 시간에 개발이 가능하며, 사용의 편의성으로 인해 많이 사용되고 있다. 특히, FPGA를 이용하여 진정한 난수 생성기를 구현하는 방법에는 여러 가지가 있지만, 홀수개의 인버터(inverter)를 이용하여 루프를 형성하고 특정 시점에서의 루프 출력을 샘플해서 사용하는 링 오실레이터(Ring-Oscillator) 방식이 대표적인 방식이다.

[5] 이와 다르게, D 플립플롭(Flip-Flop : FF)의 설정시간(setup time)과 보류시간(hold time) 특성으로 인해 발생하는 유사안정상태(metastabillty)를 이용하는 방법이 등장하였다. 이는 D 플립플롭의 D 핀과 CLK 핀에 동시에 클럭 신호를 인가하여, 두 개의 핀에 거의 동시에 같은 신호가 인가되게 하여, 두 신호가 도착하는 미세한 차이에 의해 출력되는 값이 결정되게 하는 방법이다.

[6] 최근에 제안된 방법 중에는 FPGA 칩의 내부에 있는 LUT(Look Up Table)를 활용하여 딜레이를 조절 가능한 버퍼(혹은 인버터)로 사용하는 방법이 제안되었다.

[7] 도 1 은 3개의 입력신호를 통해 2^3개의 출력을 생성해 낼 수 있는 LUT의 구조를

추상화하여 보여주고 있는 회로도로서, 도 1에서 도시하고 있는 것과 같이 LUT의 구조는 1비트를 저장할 수 있는 2^3개의 저장 공간에 있는 값을 입력 신호 I_1, I_2, I_3에 따라 각 비트를 선택하여 출력하는 구조이며, 이를 통해 다양한 로직 게이트를 구현할 수 있도록 되어 있다.

[8] 도 2 는 도 1의 구조를 활용한 딜레이 조절 가능한 버퍼를 나타낸 구성도로서, LUT의 SRAM에는 '0101 0101' 이란 값이 세팅되어 있어야 한다. 그리고 I_1 입력은 버퍼의 입력에 해당되는 부분이 되면, I_2 및 I_3와 관계없이 I_1 값에 의해 출력(O)은 '0'이 되거나 '1'이 된다. 이때 I_2 및 I_3는 출력 값에는 영향을 미치지 않지만, I_1에 의해 선택된 값이 어느 경로를 통해 출력(O)으로 전달될지를 결정하게 되며, 이는 입력 I_1으로부터 출력(O)까지의 딜레이를 변하게 하는 요소가 된다.

[9] I_2와 I_3에 의해 결정되는 경로의 수는 총 4 가지이다. 최근에 개발되는 FPGA 칩들은 입력의 수가 6 개인 LUT를 포함하기도 한다. N 개의 입력 신호를 가지는 LUT를 LUT_N 이라고 표시하며, LUT_N의 경우 PDB로 구현할 시에 2^{N-1} 개의 경로를 가지게 된다. I_1을 제외한 신호로 만들 수 있는 경로 컨트롤 신호를 I로 표기하기로 하며, $I=(I_2,I_3,...,I_N)$으로 나타낸다. 이 경로 중 가장 긴 딜레이를 가질 때의 입력 값을 I_L 이라고 표시하며, 가장 짧은 딜레이를 가질 때의 입력 값을 I_S 라고 한다. 입력이 I_L과 I_S일 때 가장 큰 딜레이 차이를 얻을 수 있으며, 이를 도 3과 같이 직렬로 여러 개를 연결하면 입력 신호에 따라 큰 딜레이 차를 만들 수 있다.

[10] 일반적으로 FPGA 칩에서 LUT를 구현함에 있어 LUT를 구성하기 위한 동일한 트랜지스터 레벨의 셀을 이용하여 제작되며, 따라서 칩 내부에서 LUT의 위치에 따른 변화는 적은 편이며, 반도체 다이(die) 내에서의 칩 위치에 따라서도 그 영향이 적은 편이다. 따라서 입력 값에 따른 딜레이에 대한 특성은 거의 모든 셀에서 유사하게 나타나는 경향이 있다.

[11] 도 4 는 위에서 설명한 PDB를 이용하여 구현한 진정한 난수 생성기를 나타낸 구성도이다. 도 4와 같이, FF의 D 입력과 CLK 입력 경로에 PDB를 직렬로 연결하여 각각 경로를 구성한다. 그리고 두 개의 경로에 배치된 PDB의 수가 같고, 경로를 동일하게 라우팅 하였다면, 두 경로에 거의 동시에 같은 클럭 신호가 인가되므로, 해당 FF에서는 상위 경로와 하위 경로의 미세한 차이에 의해 어떤 신호가 먼저 들어오느냐에 따라 FF의 출력이 0(zero)이 될 수도 있으며 1이 될 수도 있다. 만약 클럭의 상승에지(rising edge)가 상위 경로에 먼저 도착하였다면, FF의 출력은 1이 될 것이며, 하위 경로에 먼저 도착하였다면 출력은 0이 될 것이다.

[12] 도 5a 및 도 5b는 FF에서 발생할 수 있는 유사안정상태(metastabillty)에 대하여 설명하기 위한 구성도이다. 도 5a 및 도 5b와 같은 특성을 이용하여 FF을 유사안정상태로 만들면 랜덤한 비트 출력을 얻을 수 있다. 도 4에서 2진 계수기(Binary Counter)와 디코더(Decoder)는 PI-Control을 위해서 필요한

요소들이다. 2진 계수기는 FF의 출력이 1이면 증가되며, 0이면 감소되는 카운터이다. 이상적인 경우에는 카운터의 값이 0일 때 상위 경로와 하위 경로의 길이가 같기 때문에 유사안정상태가 된다. 만약 여기에서 카운터 값이 증가한다면, 증가한 카운터 값은 유사안정상태의 에러(error)로 작용하게 되며, 다시 카운터의 값이 감소하도록 상위 경로의 딜레이를 증가시키거나 하위 경로의 딜레이를 감소시켜 다시 유사안정상태로 돌리는 쪽으로 제어를 하게 된다. 또한 카운터 값이 유사안정상태에서 감소할 경우에는 상위 경로의 딜레이를 감소시키거나, 하위 경로의 딜레이를 증가시켜 다시 유사안정상태로 돌리도록 제어를 하게 된다. 이렇게 함으로써, 꾸준히 유사안정상태를 유지하도록 한다. 이때, 카운터의 형태와 디코더의 형태는 다양한 방법이 존재할 수 있으며 특정하지 않는다.

[13] 그러나 위 회로의 동작시 실제는 상위 경로와 하위 경로가 정확히 같지 않기 때문에 0이 아닌 다른 카운터 값에서 유사안정상태가 발생하며, 계속해서 PI-Control을 통해 유사안정상태를 유지하기 때문에, 유사안정상태의 카운터 값에서 증가 및 감소를 계속하며, 특정 범위의 카운터 값에서 오르락 내리락 하는 현상을 보인다.

[14] 이처럼, 기존에 제안된 PDB 및 PI-Control에 의한 FPGA기반 TRNG의 경우, PI-Control의 특성으로 인하여 앞서 설명한대로 특정 카운터 범위에서 오르락 내리락 하면서 유사안정상태를 유지한다. 이에 따라 카운터가 증감하는 범위의 가장자리 값에서는 유사안정상태의 값이 아닌 항상 고정된 값이 출력되는 문제점이 발생되게 된다. 예컨대, 카운터의 최대값에서는 항상 1을 출력하는 경향이 있으며, 최소값에서는 항상 0을 출력하는 경향이 있다. 따라서 일반적인 경우에는 이런 비-유사안정상태(non-metastable)의 출력으로 인해 얻고자 하는 랜덤 시퀀스의 획득이 어려우며, 이러한 비-유사안정상태의 출력을 제거하기 위한 필터를 사용하게 된다. 그러나 이러한 필터를 사용하게 되면, 출력 중 일부 시퀀스를 사용할 수 없게 되므로, 전체적인 처리량을 줄어들게 하며, TRNG이 효율을 떨어지게 만들게 되는 문제점이 있다.

발명의 상세한 설명

기술적 과제

[15] 따라서 본 발명은 상기와 같은 문제점을 해결하기 위해 안출한 것으로서, FPGA(Field-Programmable Gate Array)를 이용하여 랜덤한 비트 시퀀스를 생성할 때, 랜덤 특성을 향상시키고, 처리량(throughput)을 늘리기 위한 FPGA 기반된 진정한 난수 생성 장치의 성능 향상을 위한 장치 및 방법을 제공하는데 그 목적이 있다.

[16] 본 발명의 다른 목적은 필터 없이도 TRNG가 유사안정상태(metastable)에 오랫동안 머물도록하여 충분한 랜덤성(randomness)을 보장할 수 있는 FPGA 기반된 진정한 난수 생성기의 성능 향상을 위한 장치 및 방법을 제공하는데

있다.

[17] 본 발명의 또 다른 목적은 기존 진정한 난수 생성기에서 사용되는 기법의 경우 편향되어 출력되는 값을 출력되지 못하게 제거하는 것과 달리, 본 발명에서는 편향되어 출력되는 회수를 최소로 하여 랜덤성(randomness)을 보장할 수 있는 FPGA 기반된 진정한 난수 생성기의 성능 향상을 위한 장치 및 방법을 제공하는데 있다.

과제 해결 수단

[18] 상기와 같은 목적을 달성하기 위한 본 발명에 따른 랜덤성(randomness)을 보장할 수 있는 FPGA 기반된 진정한 난수 생성기의 성능 향상을 위한 장치의 특징은 플립플롭의 데이터 핀 경로와 클럭 핀 경로의 입력을 묶어서, 동시에 클럭신호를 주입하고, 각 경로의 지연시간을 피드백을 통해 제어하여 각각의 핀에 해당 신호가 도달하는 시간차에 의해 유사안정상태(metastable)한 랜덤 시퀀스를 생성하는 TRNG 모듈과, 상기 TRNG 모듈에서 출력되는 상태 정보를 저장하고, 이를 통해 TRNG 모듈의 출력을 유사안정상태(metastable)를 유지할 수 있는 시간을 제어하는 TRNG 출력 제어부를 포함하여 구성되는데 있다.

[19] 바람직하게 상기 TRNG 모듈은 랜덤 값을 출력하는 플립플롭(Flip-Flop : FF)과, 상기 플립플롭의 데이터 핀 경로와 클럭 핀 경로의 지연시간을 제어하는 PDB 경로부와, 상기 플립플롭의 출력이 1인지, 0인지에 따라 증가 또는 감소하는 카운터 값을 출력하는 2진 계수기(Binary Counter)와, 상기 2진 계수기에서 출력되는 카운터 값으로부터 피드 백 제어를 통해 데이터 핀 경로와 클럭 핀 경로의 딜레이가 같아지는 방향으로 딜레이를 조절하는 디코더를 포함하여 구성되는 것을 특징으로 하는 한다.

[20] 바람직하게 상기 TRNG 출력 제어부는 상기 TRNG 모듈의 현재 상태와 상태에 따른 출력에 대한 히스토리를 저장하는 메모리와, 상기 2진 계수기의 카운터 값에 대해 출력된 랜덤 시퀀스의 히스토리를 저장하기 위한 메모리와, 현재의 2진 계수기의 카운터 값과 현재 플립플롭의 랜덤 출력 값을 확인하여 다음 카운터 값이 어떤 값인지를 예측하는 주소 예측기와, 상기 주소 예측기에서 출력되는 해당 카운터 값의 히스토리를 확인하고, 이를 바탕으로 카운터 값이 얼마다 골고루 분포되어 있는지를 분석하는 해밍 웨이트 산출부와, 해밍 웨이트 산출부에서 분석된 정보를 이용하여 2진 계수기에서 출력되는 카운터 값이 사용할 수 있는 타임 슬롯을 배당하는 다운 카운터 이니셜라이저와, 상기 다운 카운터 이니셜라이저로부터 배당되는 타임 슬롯을 초기값으로 입력받아 매 클럭마다 값을 하나씩 감소시키는 다운 카운터와, 상기 다운 카운터에서 출력되는 값이 0이 되면 2진 계수기의 카운터 값을 갱신하는 제로 비교기를 포함하여 구성되는 것을 특징으로 한다.

[21] 바람직하게 상기 TRNG 출력 제어부는 랜덤 출력을 위한 플립플롭에서 출력이 나올 때마다 2진 계수기에서 출력되는 카운터 값을 함께 입력받아 해당

메모리의 저장소에 값을 저장할 수 있도록 메모리의 로우 인에이블 신호를 출력하는 로우 인에이블 디코더와, 주소 예측기(210)에서 예측된 카운터 값의 히스토리를 선택하여 해밍 웨이트 산출부로 출력하는 먹스를 더 포함하여 구성되는 것을 특징으로 한다.

[22] 바람직하게 상기 메모리는 캐쉬 메모리의 저장 공간으로 구성되어, 일부 상태에 대하여 출력 히스토리를 저장할 수 있도록, 각 상태의 일부 정보만을 이용하여 메모리에 히스토리를 저장하고, 상태 일부 정보만을 이용하여 이 값을 다시 회수하는 것을 특징으로 한다.

[23] 상기와 같은 목적을 달성하기 위한 본 발명에 따른 랜덤성(randomness)을 보장할 수 있는 FPGA 기반된 진정한 난수 생성기의 성능 향상을 위한 방법의 특징은 (A) 플립플롭의 데이터 핀 경로와 클럭 핀 경로의 입력을 묶어서, 동시에 클럭신호를 주입하고, 각 경로의 지연시간을 피드백을 통해 제어하여 각각의 핀에 해당 신호가 도달하는 시간차에 의해 유사안정상태(metastable)한 랜덤 시퀀스를 출력하는 단계와, (B) 상기 출력되는 랜덤 시퀀스의 상태 정보를 저장하고, 이를 통해 출력되는 랜덤 시퀀스의 출력을 유사안정상태(metastable)를 유지할 수 있는 시간을 제어하는 단계를 포함하여 이루어지는데 있다.

[24] 바람직하게 상기 (A) 단계는 PDB를 이용하여 제공되는 TOP 경로와 BOTTOM 경로를 플립플롭(Flip-Flop : FF)에 배치하는 단계와, 상기 플립플롭의 출력이 1이면 증가되고, 0이면 감소되는 카운터 값을 출력하는 단계와, 상기 출력되는 카운터 값을 바탕으로 TOP 경로와 BOTTOM 경로의 딜레이를 조절하여 각각의 핀에 해당 신호가 도달하는 시간차에 의해 유사안정상태(metastable)한 랜덤 시퀀스를 출력하는 단계를 포함하여 이루어지는 것을 특징으로 한다.

[25] 바람직하게 상기 (B) 단계는 카운터 값에 대해 출력된 랜덤 시퀀스의 히스토리를 저장하는 단계와, 현재의 카운터 값과 현재의 랜덤 출력 값을 확인하여 다음 카운터 값이 어떤 값인지를 예측하는 단계와, 상기 예측된 카운터 값의 히스토리를 선택하여 출력하고, 출력되는 해당 카운터 값의 히스토리를 바탕으로 카운터 값이 얼마다 골고루 분포되어 있는지를 분석하는 단계와, 상기 분석된 정보를 이용하여 출력되는 카운터 값이 사용할 수 있는 타임 슬롯을 배당하는 단계와, 상기 배당되는 타임 슬롯을 초기값으로 입력받아 매 클럭마다 값을 하나씩 감소시키고, 감소되는 값이 0이 되면 카운터 값을 갱신하는 단계를 포함하여 이루어지는 것을 특징으로 한다.

[26] 바람직하게 상기 카운터의 값이 양의 방향으로 커지면 출력 중 1의 비율이 높음을 의미하고, 이는 TOP 경로의 딜레이가 상대적으로 BOTTOM 경로에 비해 짧음을 의미하므로, TOP 경로의 딜레이가 길어지거나 BOTTOM 경로의 딜레이가 짧아지는 방향으로 제어하는 것을 특징으로 한다.

[27] 바람직하게 상기 분석하는 단계는 선택된 히스토리 값 산출되는 해밍 웨이트가 N개의 비트 중 1이 몇 개가 있는지를 검출하고, 해밍 웨이트가 N/2개에 가까울수록 유사안정상태(metastable)인 것을 분석하는 것을 특징으로 한다.

발명의 효과

[28] 이상에서 설명한 바와 같은 본 발명에 따른 FPGA 기반된 진정한 난수 생성기의 성능 향상을 위한 장치 및 방법은 다음과 같은 효과가 있다.

[29] 기존 난수 생성 방법의 경우 카운터 변화 추이가 매우 규칙적이고 가장자리에 있는 카운터가 등장할 경우, 이를 랜덤성을 파괴하는 요소로 인식하여 이 경우에는 출력을 하지 않았으나, 본 발명의 경우 가장 자리 카운터가 등장하는 패턴이 불규칙적이기 때문에, 이 역시 랜덤을 구성하는 요소로 흡수하여 이 경우에도 계속하여 출력을 할 수 있어, 필터 없이도 충분한 랜덤성이 보장되므로, 가장 자리 카운터 값을 필터링 함으로써 발생하는 처리량의 저하를 제거할 수 있다.

도면의 간단한 설명

[30] 도 1 은 3개의 입력신호를 통해 2^3개의 출력을 생성해 낼 수 있는 LUT의 구조를 추상화하여 보여주고 있는 회로도

[31] 도 2 는 도 1의 구조를 활용한 딜레이 조절 가능한 버퍼를 나타낸 구성도

[32] 도 3 은 도 2의 구조를 M개의 PDB를 직렬로 연결하여 나타낸 구성도

[33] 도 4 는 위에서 설명한 PDB를 이용하여 구현한 진정한 난수 생성기를 나타낸 구성도

[34] 도 5a 및 도 5b는 FF에서 발생할 수 있는 유사안정상태(metastabillty)에 대하여 설명하기 위한 구성도

[35] 도 6 은 본 발명의 실시예에 따른 FPGA 기반된 진정한 난수 생성기의 성능 향상을 위한 구성을 나타낸 블록도

[36] 도 7 은 도 1의 PDB 경로부의 구조를 상세히 나타낸 회로도

[37] 도 8 은 도 1의 PDB 경로부의 구조를 LUT3을 이용하여 나타낸 실시예

[38] 도 9 는 도 8의 LUT3의 구조도를 나타낸 실시예

[39] 도 10a 및 도 10b는 각 카운터별로 1이 출력되는 확률을 제안한 방법과 기존의 방법에 대하여 나타낸 그래프

[40] 도 11a 및 도 11b는 전체 분포 중에서 각 카운터가 몇 번 등장했는지를 비율로 나타낸 그래프

[41] 도 12a 및 도 12b는 기간에 따른 카운터 값의 변화 추이를 나타낸 그래프

발명의 실시를 위한 최선의 형태

[42] 본 발명의 다른 목적, 특성 및 이점들은 첨부한 도면을 참조한 실시예들의 상세한 설명을 통해 명백해질 것이다.

[43] 본 발명에 따른 FPGA 기반된 진정한 난수 생성기의 성능 향상을 위한 장치 및 방법의 바람직한 실시예에 대하여 첨부한 도면을 참조하여 설명하면 다음과 같다. 그러나 본 발명은 이하에서 개시되는 실시예에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 본 실시예는 본 발명의 개시가 완전하도록하며 통상의 지식을 가진자에게 발명의 범주를 완전하게 알려주기

위해 제공되는 것이다. 따라서 본 명세서에 기재된 실시예와 도면에 도시된 구성은 본 발명의 가장 바람직한 일 실시예에 불과할 뿐이고 본 발명의 기술적 사상을 모두 대변하는 것은 아니므로, 본 출원시점에 있어서 이들을 대체할 수 있는 다양한 균등물과 변형예들이 있을 수 있음을 이해하여야 한다.

[44] 도 6 은 본 발명의 실시예에 따른 FPGA 기반된 진정한 난수 생성기의 성능 향상을 위한 구성을 나타낸 블록도이다.

[45] 도 6과 같이, 진정한 난수 생성기(TRNG)는 PDB(Physical Data Base)와 PI 컨트롤을 이용해 랜덤 시퀀스를 생성하는 TRNG 모듈(100)과, TRNG 모듈(100)에서 출력되는 스트림과 현재의 카운터 값을 저장하고, 이를 바탕으로 TRNG 모듈(100)의 출력을 제어하는 TRNG 출력 제어부(200)로 구성된다.

[46] 상기 TRNG 모듈(100)은 PDB를 이용하여 TOP 경로와 BOTTOM 경로를 제공하는 PDB 경로부(110)를 구성하고, 상기 PDB 경로부(110)의 다음 단에는 플립플롭(Flip-Flop : FF)(120)을 배치한다. 그리고 상기 FF(120)의 출력이 1이면 증가되고, 0이면 감소되는 카운터 값을 출력하는 2진 계수기(Binary Counter)(140)와, 2진 계수기(140)에서 출력되는 카운터 값을 바탕으로 하여 PDB 경로부(110)의 TOP 경로와 BOTTOM 경로의 딜레이를 조절하는 디코더(130)로 구성된다.

[47] 상기 TRNG 출력 제어부(200)는 상기 2진 계수기(140)의 카운터 값에 대해 출력된 랜덤 시퀀스의 히스토리를 저장하기 위한 메모리(250)와, 랜덤 출력을 위한 FF(120)에서 출력이 나올 때마다 2진 계수기(140)에서 출력되는 카운터 값을 함께 입력받아 해당 메모리(250)의 저장소에 값을 저장할 수 있도록 메모리(250)의 로우 인에이블 신호를 출력하는 로우 인에이블 디코더(240)와, 현재의 2진 계수기(140)의 카운터 값과 현재 FF(120)의 랜덤 출력 값을 확인하여 다음 카운터 값이 어떤 값인지를 예측하는 주소 예측기(210)와, 주소 예측기(210)에서 예측된 카운터 값의 히스토리를 선택하여 출력하는 먹스(MUX)(260)와, 먹스(260)를 통해 출력되는 해당 카운터 값의 히스토리를 확인하고, 이를 바탕으로 카운터 값이 얼마다 골고루 분포되어 있는지를 분석하는 해밍 웨이트 산출부(hamming weight calculator)(270)와, 해밍 웨이트 산출부(270)에서 분석된 정보를 이용하여 2진 계수기(140)에서 출력되는 카운터 값이 사용할 수 있는 타임 슬롯을 배당하는 다운 카운터 이니셜라이저(280)와, 다운 카운터 이니셜라이저(280)로부터 배당되는 타임 슬롯을 초기값으로 입력받아 매 클럭마다 값을 하나씩 감소시키는 다운 카운터(230)와, 다운 카운터(230)에서 출력되는 값이 0이 되면 인에이블(EN) 신호를 활성화하여 2진 계수기(140)의 카운터 값을 갱신하는 제로 비교기(220)로 구성된다.

[48] 도 7 은 도 1의 PDB 경로부의 구조를 상세히 나타낸 회로도이다.

[49] 도 7과 같이, PDB 경로부(110)는 PDB(111)를 여러 개 직렬로 연결하여 상위에 TOP 경로(112)를 구성하고, 하위에 BOTTOM 경로(113)를 구성한다. 그리고 PBD의 딜레이 경로(112)(113)는 각각의 PDB(111)의 딜레이 조절 신호(116)에

의해 전체 경로의 딜레이를 조절할 수 있다. 상기 각각의 딜레이 조절 신호(116)는 묶어서 TOP 경로(112)의 컨트롤 신호(114)와 BOTTOM 경로(113)의 컨트롤 신호(115)로 사용되며, 이는 디코더(130)에 연결되어 TOP 경로(112)와 BOTTOM 경로(113)의 딜레이는 디코더(130)로부터 컨트롤되게 된다.

[50] 도 8 은 도 1의 PDB 경로부의 구조를 LUT3을 이용하여 나타낸 실시예이고, 도 9 는 도 8의 LUT3의 구조도를 나타낸 실시예이다.

[51] 도 8과 같이, LUT3은 FPGA 칩에서 제공하는 3-input LUT(Look Up Table)이다. LUT는 FPGA를 구성하는 기본요소 중 하나이며, 칩의 구성에 필요한 조합 회로를 구성하기 위해 활용된다. 이를 활용하면 딜레이 조절이 가능한 버퍼를 만드는 것이 가능하다.

[52] 도 9를 참조하여 LUT3의 구조적 원리를 설명하면, LUT의 입력이 X개(111-1, 111-2, 111-3)라고 하면, LUTX는 2^X개의 SRAM 저장공간(111-6)을 가진다. 이 값은 X 단계의 먹스(111-5)를 통해 출력 O(111-4)로 출력이 된다. 이때, SRAM 저장공간(111-6)의 값을 '1010 1010'으로 설정을 하고, 입력 I_1(111-1), I_2(111-2), 그리고 I_3(111-3)를 조절하면, 각각의 SRAM 주소에 있는 값을 출력 O(111-4)를 통해 출력할 수 있다. 이때, 출력이 0이 될지 1이 될지는 입력 I_1(111-1)을 통해서 결정되며, I_2(111-2)와 I_3(111-3)는 출력되는 값에는 영향을 미치지 않는다. 즉, 입력 I_1(111-1)이 0이면 출력은 0이되고, 1이면 출력은 1이 되므로 버퍼와 같은 형태가 된다. 다만, 입력 I_2(111-2)와 I_3(111-3)는 출력 값에는 영향을 미치지 못하더라도, 각 SRAM에서 출력된 값이 출력되는 경로를 다르게 하는 요인이 된다. I_2(111-2), I_3(111-3)에 의해 결정되는 경로는 거의 같은 길이를 가진다 해도, 물리적으로 미세한 차이의 경로차가 발생하기 마련이며, 이는 버퍼의 입력으로부터 출력에 이르기 까지 값이 통과하는 시간에 영향을 줄 수 있다. 이를 심볼화하여 나타낸 것이 도 8이다. 이러한 딜레이를 조절 가능한 버퍼를 도 8과 같이 형상화 할 수 있다.

[53] 상기 플립플롭(FF)(120)은 일반적인 D 플립플롭이다. 이때, D핀의 입력은 PDB 경로부(110)의 TOP 경로(112)가 연결되며, CLK핀의 입력은 BOTTOM 경로(113)가 연결된다. 그리고 PDB 경로부(110)의 TOP 경로(112)와 BOTTOM 경로(113)의 입력 핀은 함께 묶이며, 이 핀을 통해 클럭 신호를 공급받게 된다. 또한 TOP 경로(112)와 BOTTOM 경로(113)의 길이가 거의 같다면, FF(120)에 클럭의 상승에지가 도착하는 시간은 거의 같다고 할 수 있다. 클럭의 상승에지에서 값이 변화하는 FF(120)을 사용한다고 하면, 상승에지가 TOP 경로(112)를 통해 먼저 입력된 경우에는 FF(120)의 출력은 1이 되며, 반대의 경우 출력은 0이 된다.

[54] 상기 2진 계수기(140)는 FF(120)의 출력에 따라 값이 증/감 한다. 만약 FF(120)의 출력이 1일 경우 카운터의 값은 증가하며, 반대의 경우 감소한다. 카운터의 값은 부호 비트를 따로 두어 사용할 수도 있으며, 2의 보수 형태로 음수를 표현할 수도 있으며, 구현에 제한을 두지 않는다. 음수 표현 방법은 디코더(130)의 설계에

영향을 미치며, 일반적으로 하드웨어로 구현 시에는 부호 비트를 두는 것이 디코더(130)를 구현하기에 수월함이 있다.

[55] 상기 디코더(130)는 2진 계수기(140)로부터 전달된 카운터(부호 비트가 있는 경우 이 역시 포함) 값을 PDB 경로부(110)내의 TOP 경로(112)와 BOTTOM 경로(113)의 딜레이를 조절할 수 있는 신호로 변환하는 일을 한다. 카운터의 값이 양의 방향으로 커지면 이는 출력 중 1의 비율이 높음을 의미하고, 이는 TOP 경로(112)의 딜레이가 상대적으로 BOTTOM 경로(113)에 비해 짧음을 의미하므로, TOP 경로(112)의 딜레이가 길어지거나 BOTTOM 경로(113)의 딜레이가 짧아지는 방향으로 PDB(111)들을 제어할 수 있는 신호를 출력한다. 반대의 경우 TOP 경로(112)의 딜레이가 짧아지거나, BOTTOM 경로(113)의 딜레이가 길어지는 방향으로 제어신호를 출력한다.

[56] 상기 메모리(250)는 N x M의 플립플롭(252)으로 구성되어 히스토리를 저장한다. 이때 N은 각 카운터당 저장되는 출력의 히스토리 개수이며, M은 카운터의 개수이다. 2진 계수기(140)의 부호를 포함한 카운터의 비트 길이를 C 비트라고 하였을 때, M은 2^C개로 구성되어야 한다. 하지만 이 경우 저장 장소가 필요 이상으로 많이 필요하게 된다. 하지만, 실제 TRNG를 구하면, 카운터의 값이 PI 제어에 의해 특정 값으로 수렴하고 난 뒤에 해당 값의 특정 범위를 오르락내리락 하는 것을 반복하기 때문에, 그렇게 많은 저장공간이 필요하지 않는다는 점을 발견하였다. 따라서 본 발명에서는 캐쉬 메모리 형태의 저장공간을 제안한다. 실제 필요한 저장공간의 개수는 수렴 이후 값이 변하는 범위의 크기면 충분한다. 이 크기를 P라고 하였을 때, M을 P로 설정하고, 로우 인에이블 디코더(240)는 2진 계수기(140)에서 출력되는 카운터 값 중 LSB(Least Significant Bit) $\log_2 P$ 개만을 입력으로 받아 해당되는 주소에 히스토리를 저장한다. TRNG의 동작 초기에는 주로 카운터가 초기값으로부터 수렴치까지 꾸준히 증가하는 추세를 보이므로, 캐쉬 형태의 저장공간으로 인해 잘못된 히스토리가 저장될 수도 있지만, 일단 수렴한 이후로는 해당 변화 범위 내에서 제대로 된 정보로 다시 갱신되므로, 이는 큰 문제 사항이 되지 않는다. 각 플립플롭(252)은 N개씩 묶어 각 카운터에 해당하는 저장소(251)로 사용하게 된다. 이 부분은 도 6에서 오른쪽 쉬프터(right shifter) 형태의 저장소로 구성이 되며, 가장 왼쪽 FF(251)에 값이 입력되면, 원래 저장되어 있던 값들이 오른쪽으로 한 비트씩 이동이 일어나고 가장 오른쪽에 있는 값은 버려지는 형태이다. 이런 식으로 각 카운터에 대한 출력 히스토리를 기억할 수 있다.

[57] 상기 주소 예측기(210)는 현재의 FF(120)의 출력 값과 2진 계수기(140)의 카운터 값을 이용해 다음 2진 계수기(140)의 값이 어떤 값이 될지를 예측하는 일을 한다. 이는 이미 2진 계수기(140) 내부에서 다음 카운터 값을 결정하기 위해 사용되고 있는 로직으로 구성될 수 있다. 따라서 주소 예측기(210)는 2진 계수기(140) 내부의 로직을 사용하거나, 도 6과 같이 별도의 로직을 구성하여 사용할 수 있다. 또한 주소 예측기(210)는 다음 변경될 카운터 값에 타임

슬롯(time slot)을 할당하기 위해 저장된 출력 히스토리 중에서 다음 변경될 카운터의 것을 가져오기 위해서 필요한 부분이다.

[58] 상기 주소 예측기(210)를 통해 예상된 주소는 LSB $\log_2 P$ 비트만을 이용하여 다시 P개의 카운터 값 중 하나를 추출하는데 사용되며, 이는 메모리(250) 아래에 있는 N개의 먹스(260)로 공급되어 P개의 출력 중 하나를 선택하는데 사용된다. 그리고 선택된 히스토리 값은 해밍 웨이트 산출부(hamming weight calculator)(270)로 공급하여 해밍 웨이트를 산출한다. 상기 해밍 웨이트는 N개의 비트 중 1이 몇 개가 있는지를 나타내는 척도이다. 따라서 해밍 웨이트가 N/2개에 가까울수록 유사안정상태(metastable)인 셈이다.

[59] 상기 다운 카운터 이니셜라이저(280)는 이러한 특성을 이용하여 해밍 웨이트를 다음 카운터에 배당한 타임 슬롯의 개수로 디코딩을 한다. 즉, 해밍 웨이트가 N/2에 가까우면 큰 타임 슬롯으로 변환하고, 그렇지 않을 경우 작은 값을 변환한다. 변환된 값은 다운 카운터(230)에 공급되며, 이 값은 매 클럭마다 줄어들게 된다.

[60] 상기 제로 비교기(220)는 단순 비교기로서 다운 카운터(230)의 값이 0인지를 판단하여, 0일 경우에만 2진 계수기(140)에 인에이블 신호를 활성화하여 카운터가 갱신되게 된다.

[61] 이와 같이 구성됨에 따라, 본 발명은 FPGA(Field-Programmable Gate Array)를 이용하여 랜덤한 비트 시퀀스를 생성할 때, 랜덤 특성을 향상시키고, 처리량(throughput)을 늘리기 위한 FPGA 기반된 진정한 난수 생성 장치의 성능 향상을 제공할 수 있게 되며, 이를 실험결과를 통해 다음과 같이 확인할 수 있다.

[62] 도 10a는 각 카운터별로 1이 출력되는 확률을 제안한 방법을, 도 10b는 각 카운터별로 1이 출력되는 확률을 기존의 방법에 대하여 나타낸 그래프이다. 도 10a 및 도 10b에서 확률이 0.5에 가까울수록 유사안정상태(metastable)로 출력을 내는 카운터가 되는 것이며, 확률이 0에 가까우면 0을 출력하는 빈도가 높거나, 1에 가까우면 1을 출력하는 빈도가 높은 카운터 값임을 의미한다. 그리고 도 11a는 제안한 방법을 적용하였을 때, 전체 분포 중에서 각 카운터가 몇 번 등장했는지를 비율로 나타낸 그래프이고, 도 11b는 기존의 방법을 적용하였을 때, 전체 분포 중에서 각 카운터가 몇 번 등장했는지를 비율로 나타낸 그래프이다.

[63] 도면을 살펴보면, 도 10b와 같이 기존의 방법의 경우 확률이 0.4~0.6 사이에 있는 카운터는 118, 120, 121 정도로 정리할 수 있다. 이들 카운터의 등장 확률을 도 11b에서 살펴보면, 대략 0.15~0.25 사이에서 분포되어 있음을 확인할 수 있다. 대략 이들의 합은 0.6 정도 된다.

[64] 한편, 도 10a와 같이 본 발명의 경우 확률이 0.4~0.6 사이에 분포하고 있는 카운터는 434, 437, 438로 정의할 수 있으며, 도 11a에서 살펴보면, 각각 대략 0.15, 0.25, 0.35의 등장 비율을 보이고 있다. 이들의 합은 대략 0.75 정도로 기존 방법보다 랜덤한 수의 비율이 높음을 확인할 수 있다.

[65] 도 12a 및 도 12b는 기간에 따른 카운터 값의 변화 추이를 나타낸 그래프로서, 도 12a는 기존 방법의 카운터 변화 추이를 나타낸 그래프이고, 도 12b는 본 발명의 카운터 변화 추이를 나타낸 그래프이다.

[66] 도 12a를 살펴보면, 카운터가 매우 규칙적으로 112~125 사이의 구간을 오르락 내리락 하는 것을 살필 수 있으며, 도 12b를 살펴보면, 출력이 438 주변으로 집중되어 있으며, 434 주변에서도 간헐적으로 집중해서 출력되고 있음을 확인할 수 있다. 또한 출력 범위의 가장자리(430과 441) 카운터 출력 빈도가 기존 방법에 비해 훨씬 적다는 것을 그래프를 통해서 확인할 수 있다. 무엇보다 중요한 것은 기존 방법의 경우 카운터 변화 추이가 매우 규칙적이고 가장자리에 있는 카운터가 등장할 경우 이를 랜덤성을 파괴하는 요소로 인식하여 이 경우에는 출력을 하지 않는 다는 점이다. 그러나 제안 방법에서는 가장 자리 카운터가 등장하는 패턴이 불규칙적이기 때문에, 이 역시 랜덤을 구성하는 요소로 흡수하여, 이 경우에도 계속하여 출력을 할 수 있으므로, 가장 자리 카운터 값을 필터링 함으로써 발생하는 처리량의 저하가 없게 된다.

[67] 한편, 본 발명의 실시예는 컴퓨터에서 실행될 수 있는 프로그램으로 작성가능하다. 즉, 본 발명에 따른 방법에 포함된 여러 단계들은 컴퓨터로 읽을 수 있는 기록매체에 저장될 수 있다. 상기 매체는 마그네틱 저장매체(예: 롬, 플로피 디스크, 하드 디스크 등), 광학적 판독매체(예: CD-ROM, DVD), 디지털 저장매체(예: USB 메모리, 메모리 카드(SD, CF, MS, XD) 등) 및 캐리어 웨이브(예: 인터넷을 통한 전송)와 같은 기록매체를 포함한다.

[68]

[69] 상기에서 설명한 본 발명의 기술적 사상은 바람직한 실시예에서 구체적으로 기술되었으나, 상기한 실시예는 그 설명을 위한 것이며 그 제한을 위한 것이 아님을 주의하여야 한다. 또한, 본 발명의 기술적 분야의 통상의 지식을 가진자라면 본 발명의 기술적 사상의 범위 내에서 다양한 실시예가 가능함을 이해할 수 있을 것이다. 따라서 본 발명의 진정한 기술적 보호 범위는 첨부된 특허청구범위의 기술적 사상에 의해 정해져야 할 것이다.

청구범위

[청구항 1] 플립플롭의 데이터 핀 경로와 클럭 핀 경로의 입력을 묶어서, 동시에 클럭신호를 주입하고, 각 경로의 지연시간을 피드백을 통해 제어하여 각각의 핀에 해당 신호가 도달하는 시간차에 의해 유사안정상태(metastable)한 랜덤 시퀀스를 생성하는 TRNG 모듈과,
상기 TRNG 모듈에서 출력되는 상태 정보를 저장하고, 이를 통해 TRNG 모듈의 출력을 유사안정상태(metastable)를 유지할 수 있는 시간을 제어하는 TRNG 출력 제어부를 포함하여 구성되는 것을 특징으로 하는 FPGA 기반된 진정한 난수 생성기의 성능 향상을 위한 장치.

[청구항 2] 제 1 항에 있어서, 상기 TRNG 모듈은
랜덤 값을 출력하는 플립플롭(Flip-Flop : FF)과,
상기 플립플롭의 데이터 핀 경로와 클럭 핀 경로의 지연시간을 제어하는 PDB 경로부와,
상기 플립플롭의 출력이 1인지, 0인지에 따라 증가 또는 감소하는 카운터 값을 출력하는 2진 계수기(Binary Counter)와,
상기 2진 계수기에서 출력되는 카운터 값으로부터 피드 백 제어를 통해 데이터 핀 경로와 클럭 핀 경로의 딜레이가 같아지는 방향으로 딜레이를 조절하는 디코더를 포함하여 구성되는 것을 특징으로 하는 FPGA 기반된 진정한 난수 생성기의 성능 향상을 위한 장치.

[청구항 3] 제 2 항에 있어서, 상기 TRNG 출력 제어부는
상기 TRNG 모듈의 현재 상태와 상태에 따른 출력에 대한 히스토리를 저장하는 메모리와,
상기 2진 계수기의 카운터 값에 대해 출력된 랜덤 시퀀스의 히스토리를 저장하기 위한 메모리와,
현재의 2진 계수기의 카운터 값과 현재 플립플롭의 랜덤 출력 값을 확인하여 다음 카운터 값이 어떤 값인지를 예측하는 주소 예측기와,
상기 주소 예측기에서 출력되는 해당 카운터 값의 히스토리를 확인하고, 이를 바탕으로 카운터 값이 얼마다 골고루 분포되어 있는지를 분석하는 해밍 웨이트 산출부와,
해밍 웨이트 산출부에서 분석된 정보를 이용하여 2진 계수기에서 출력되는 카운터 값이 사용할 수 있는 타임 슬롯을 배당하는 다운 카운터 이니셜라이저와,
상기 다운 카운터 이니셜라이저로부터 배당되는 타임 슬롯을

초기값으로 입력받아 매 클럭마다 값을 하나씩 감소시키는 다운 카운터와,
상기 다운 카운터에서 출력되는 값이 0이 되면 2진 계수기(140)의 카운터 값을 갱신하는 제로 비교기를 포함하여 구성되는 것을 특징으로 하는 FPGA 기반된 진정한 난수 생성기의 성능 향상을 위한 장치.

[청구항 4] 제 3 항에 있어서, 상기 TRNG 출력 제어부는
랜덤 출력을 위한 플립플롭에서 출력이 나올 때마다 2진 계수기에서 출력되는 카운터 값을 함께 입력받아 해당 메모리의 저장소에 값을 저장할 수 있도록 메모리의 로우 인에이블 신호를 출력하는 로우 인에이블 디코더와,
주소 예측기(210)에서 예측된 카운터 값의 히스토리를 선택하여 해밍 웨이트 산출부로 출력하는 먹스를 더 포함하여 구성되는 것을 특징으로 하는 FPGA 기반된 진정한 난수 생성기의 성능 향상을 위한 장치.

[청구항 5] 제 2 항에 있어서, 상기 PDB 경로부는
PDB를 여러 개 직렬로 연결하여 상위에 TOP 경로를 구성하고, 하위에 BOTTOM 경로를 구성하며,
FPGA 칩 내부에 있는 LUT(Look Up Table)의 입력 제어를 통해 딜레이를 조절 가능한 버퍼 및 인버터를 포함하는 것을 특징으로 하는 FPGA 기반된 진정한 난수 생성기의 성능 향상을 위한 장치.

[청구항 6] 제 2 항에 있어서,
상기 플립플롭은 D 플립플롭인 것을 특징으로 하는 FPGA 기반된 진정한 난수 생성기의 성능 향상을 위한 장치.

[청구항 7] 제 6 항에 있어서,
상기 플립플롭은 D핀의 입력이 PDB 경로부의 TOP 경로로 연결되고, CLK핀의 입력이 BOTTOM 경로로 연결되며, 상기 TOP 경로와 BOTTOM 경로의 입력 핀이 함께 묶여 클럭 신호를 공급받게 되는 것을 특징으로 하는 FPGA 기반된 진정한 난수 생성기의 성능 향상을 위한 장치.

[청구항 8] 제 2 항에 있어서,
상기 메모리는 캐쉬 메모리의 저장공간으로 구성되어, 일부 상태에 대하여 출력 히스토리를 저장할 수 있도록, 각 상태의 일부 정보만을 이용하여 메모리에 히스토리를 저장하고, 상태 일부 정보만을 이용하여 이 값을 다시 회수하는 것을 특징으로 하는 FPGA 기반된 진정한 난수 생성기의 성능 향상을 위한 장치.

[청구항 9] 제 2 항에 있어서,
상기 주소 예측기는 2진 계수기 내부의 로직을 사용하거나, 별도의

로직을 구성하여 사용하는 것을 특징으로 하는 FPGA 기반된 진정한 난수 생성기의 성능 향상을 위한 장치.

[청구항 10] 제 2 항에 있어서,
상기 다운 카운터 이니셜라이저는 해밍 웨이트를 다음 카운터에 배당한 타임 슬롯의 개수로 디코딩하는 것을 특징으로 하는 FPGA 기반된 진정한 난수 생성기의 성능 향상을 위한 장치.

[청구항 11] (A) 플립플롭의 데이터 핀 경로와 클럭 핀 경로의 입력을 묶어서, 동시에 클럭신호를 주입하고, 각 경로의 지연시간을 피드백을 통해 제어하여 각각의 핀에 해당 신호가 도달하는 시간차에 의해 유사안정상태(metastable)한 랜덤 시퀀스를 출력하는 단계와,
(B) 상기 출력되는 랜덤 시퀀스의 상태 정보를 저장하고, 이를 통해 출력되는 랜덤 시퀀스의 출력을 유사안정상태(metastable)를 유지할 수 있는 시간을 제어하는 단계를 포함하여 이루어지는 것을 특징으로 하는 FPGA 기반된 진정한 난수 생성기의 성능 향상을 위한 방법.

[청구항 12] 제 11 항에 있어서, 상기 (A) 단계는
PDB를 이용하여 제공되는 TOP 경로와 BOTTOM 경로를 플립플롭(Flip-Flop : FF)에 배치하는 단계와,
상기 플립플롭의 출력이 1이면 증가되고, 0이면 감소되는 카운터 값을 출력하는 단계와,
상기 출력되는 카운터 값을 바탕으로 TOP 경로와 BOTTOM 경로의 딜레이를 조절하여 각각의 핀에 해당 신호가 도달하는 시간차에 의해 유사안정상태(metastable)한 랜덤 시퀀스를 출력하는 단계를 포함하여 이루어지는 것을 특징으로 하는 FPGA 기반된 진정한 난수 생성기의 성능 향상을 위한 방법.

[청구항 13] 제 11 항에 있어서, 상기 (B) 단계는
카운터 값에 대해 출력된 랜덤 시퀀스의 히스토리를 저장하는 단계와,
현재의 카운터 값과 현재의 랜덤 출력 값을 확인하여 다음 카운터 값이 어떤 값인지를 예측하는 단계와,
상기 예측된 카운터 값의 히스토리를 선택하여 출력하고,
출력되는 해당 카운터 값의 히스토리를 바탕으로 카운터 값이 얼마다 골고루 분포되어 있는지를 분석하는 단계와,
상기 분석된 정보를 이용하여 출력되는 카운터 값이 사용할 수 있는 타임 슬롯을 배당하는 단계와,
상기 배당되는 타임 슬롯을 초기값으로 입력받아 매 클럭마다 값을 하나씩 감소시키고, 감소되는 값이 0이 되면 카운터 값을 갱신하는 단계를 포함하여 이루어지는 것을 특징으로 하는 FPGA

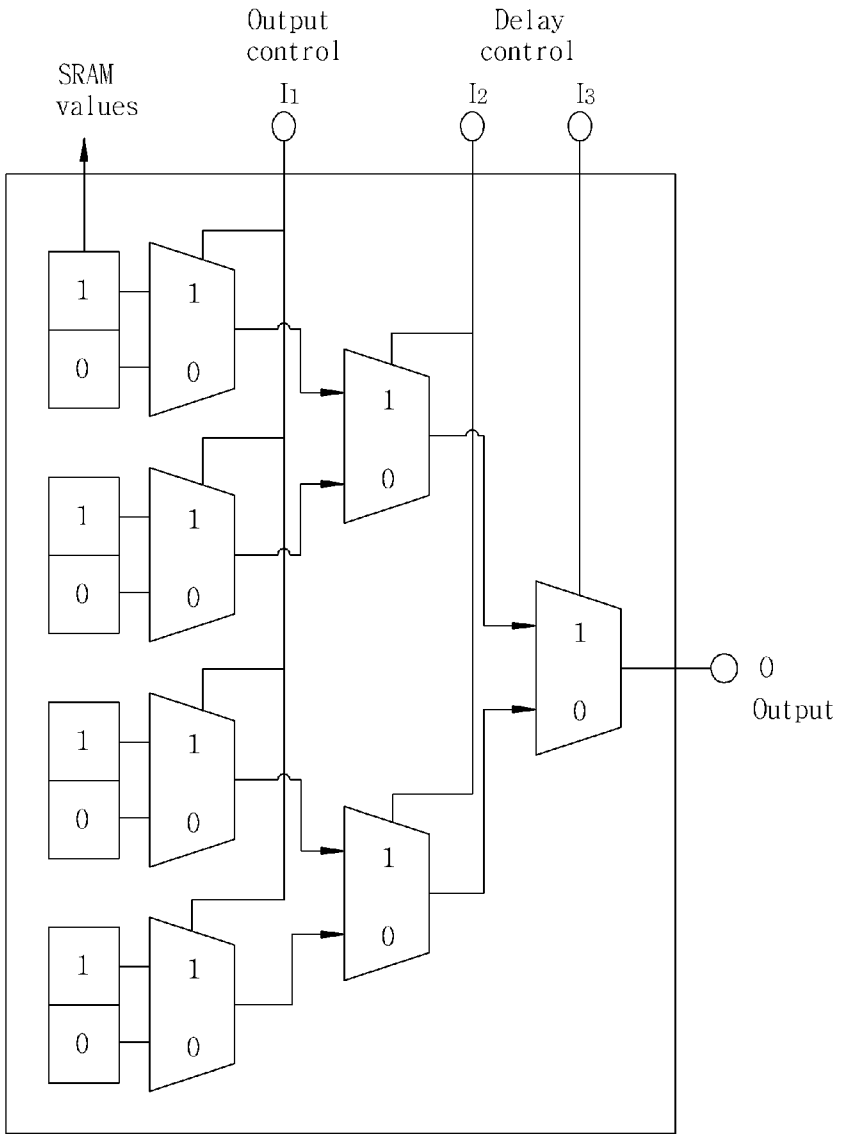
기반된 진정한 난수 생성기의 성능 향상을 위한 방법.

[청구항 14] 제 13 항에 있어서,
상기 카운터의 값이 양의 방향으로 커지면 출력 중 1의 비율이 높음을 의미하고, 이는 TOP 경로의 딜레이가 상대적으로 BOTTOM 경로에 비해 짧음을 의미하므로, TOP 경로의 딜레이가 길어지거나 BOTTOM 경로의 딜레이가 짧아지는 방향으로 제어하는 것을 특징으로 하는 FPGA 기반된 진정한 난수 생성기의 성능 향상을 위한 방법.

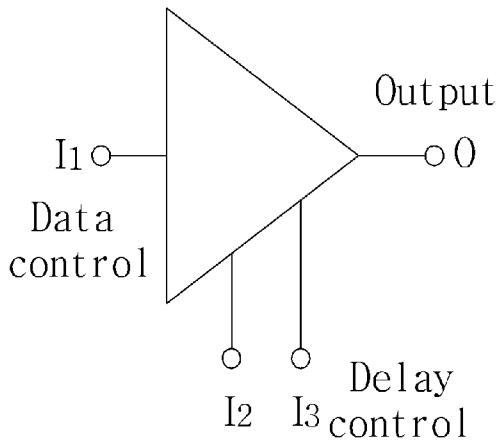
[청구항 15] 제 13 항에 있어서,
상기 분석하는 단계는 선택된 히스토리 값 산출되는 해밍 웨이트가 N개의 비트 중 1이 몇 개가 있는지를 검출하고, 해밍 웨이트가 N/2개에 가까울수록 유사안정상태(metastable)인 것을 분석하는 것을 특징으로 하는 FPGA 기반된 진정한 난수 생성기의 성능 향상을 위한 방법.

[청구항 16] 제 11 항 내지 제 15 항 중 어느 하나에 의한 FPGA 기반된 진정한 난수 생성기의 성능 향상을 위한 방법의 각 단계를 실행하기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

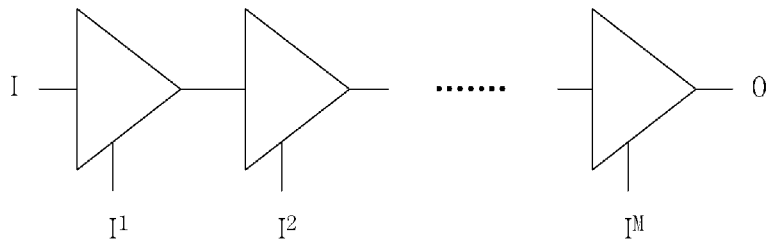
[Fig. 1]


Output control
Delay control
SRAM values
I1
I2
I3
1
0
O
Output

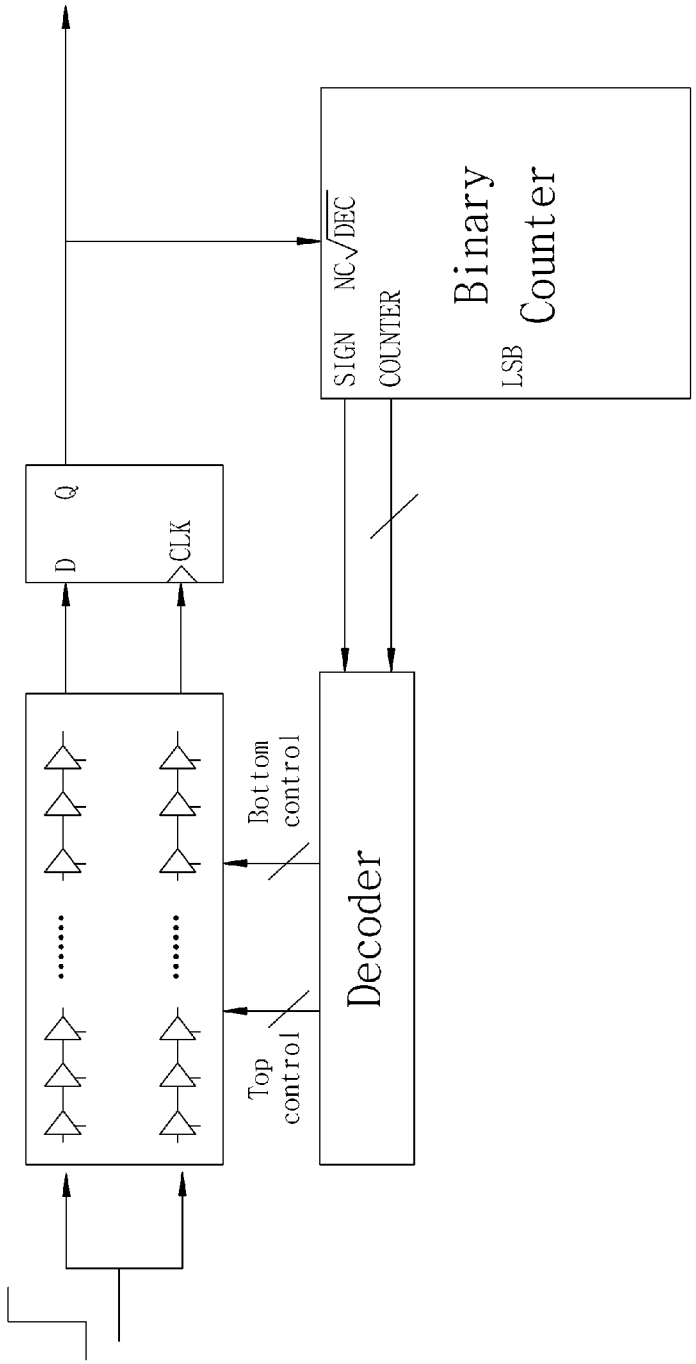
[Fig. 2]


Output
I1
O
Data control
I2
I3
Delay control

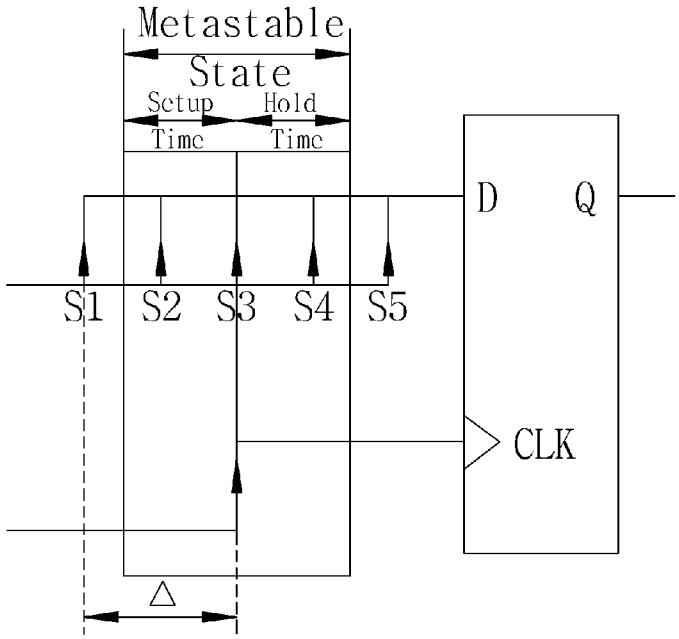
[Fig. 3]


I
O
I1
I2
IM

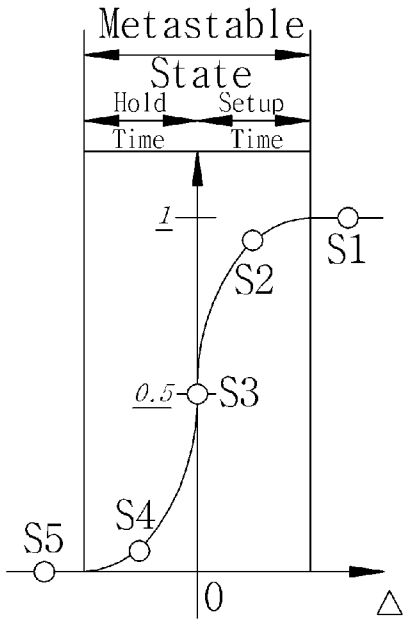
[Fig. 4]


Binary Counter
SIGN
NC/DEC
COUNTER
LSB
D
Q
CLK
Decoder
Bottom control
Top control

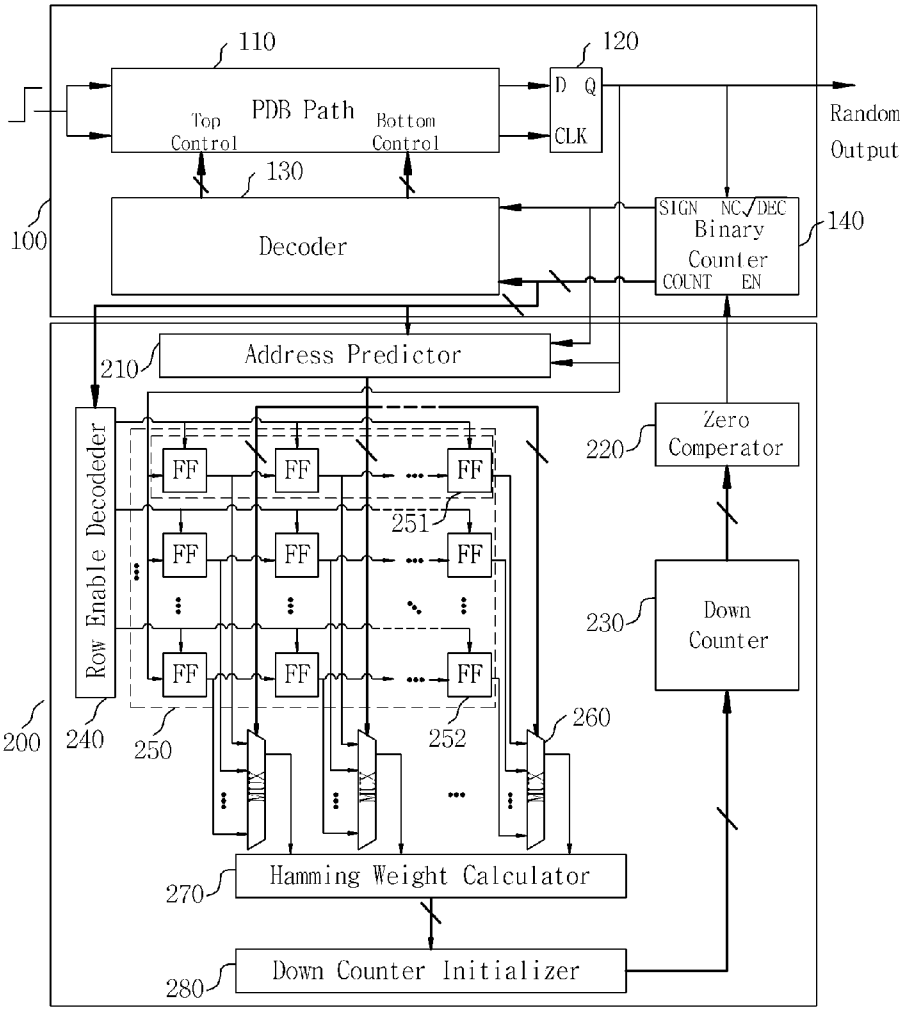
[Fig. 5a]


Metastable
State
Setup
Time
Hold
Time
D
Q
S1
S2
S3
S4
S5
CLK
△

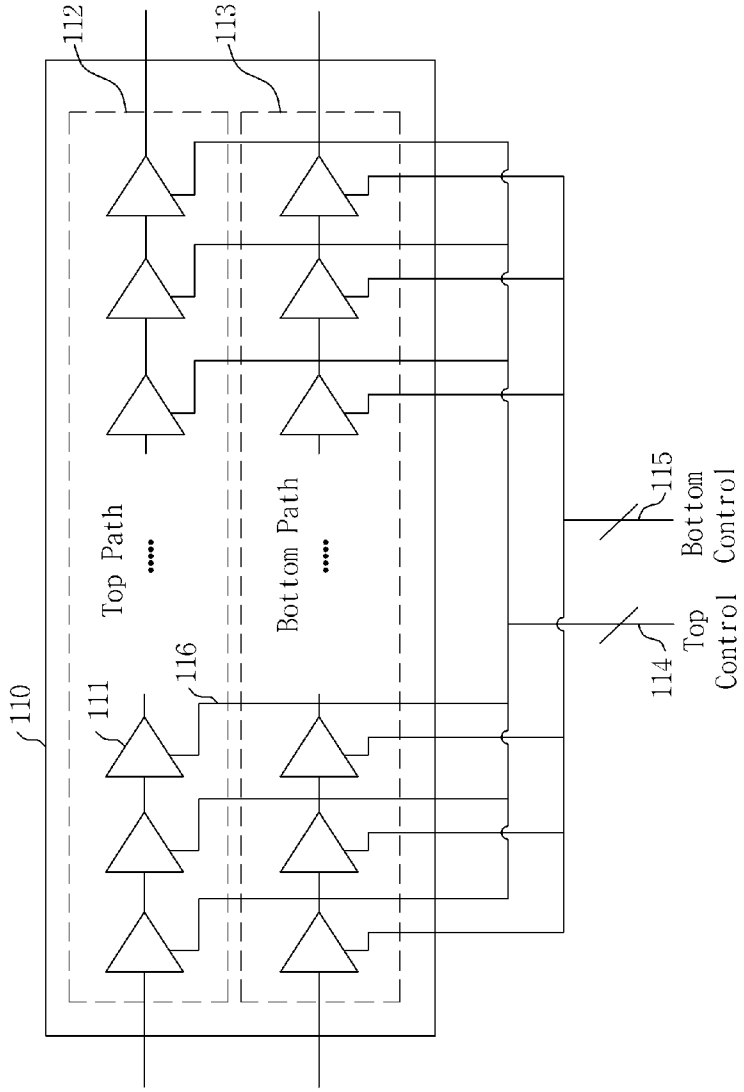
[Fig. 5b]


Metastable
State
Hold
Time
Setup
Time
1
0.5
S1
S2
S3
S4
S5
0
△

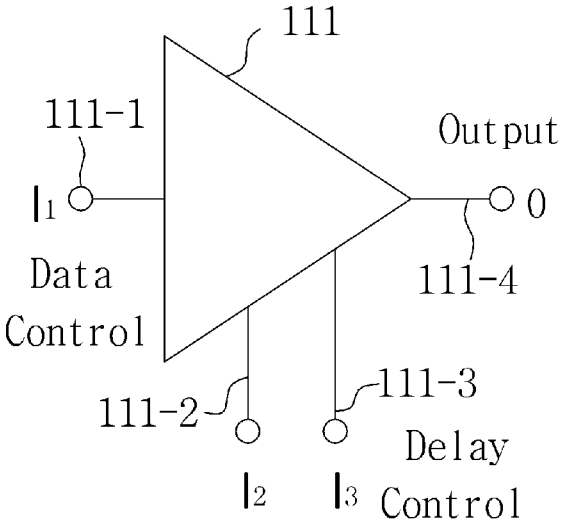
[Fig. 6]


110
120
PDB Path
Top Control
Bottom Control
D Q
CLK
Random Output
130
100
Decoder
SIGN NC/DEC
Binary Counter
COUNT EN
140
Address Predictor
210
Row Enable Decodeder
FF
251
Zero Comperator
220
Down Counter
230
200
240
250
252
260
Hamming Weight Calculator
270
Down Counter Initializer
280

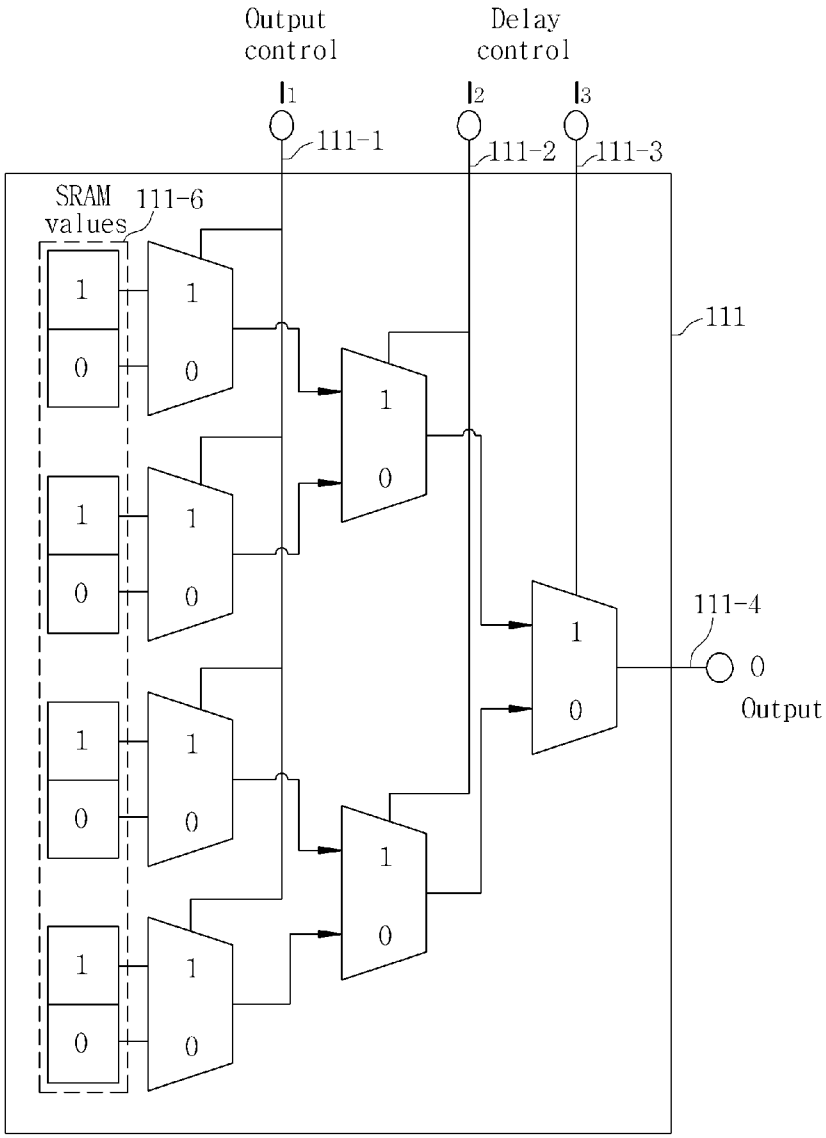
[Fig. 7]


110
111
112
113
114
115
116
Top Path
Bottom Path
Top Control
Bottom Control

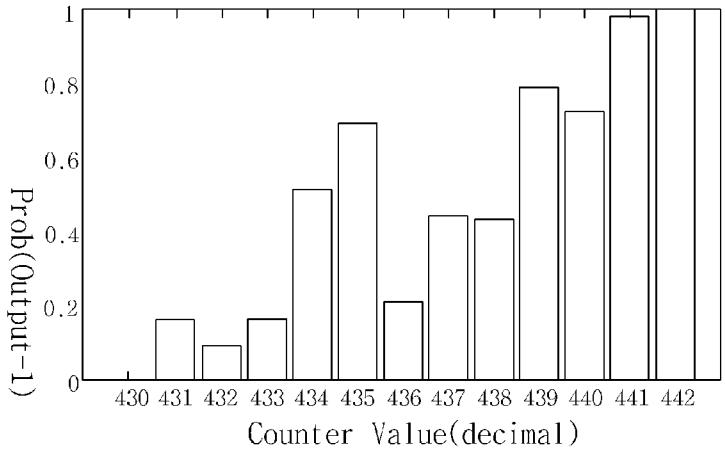
[Fig. 8]


111
111-1
I1
Data Control
Output
O
111-4
111-2
I2
111-3
I3
Delay Control

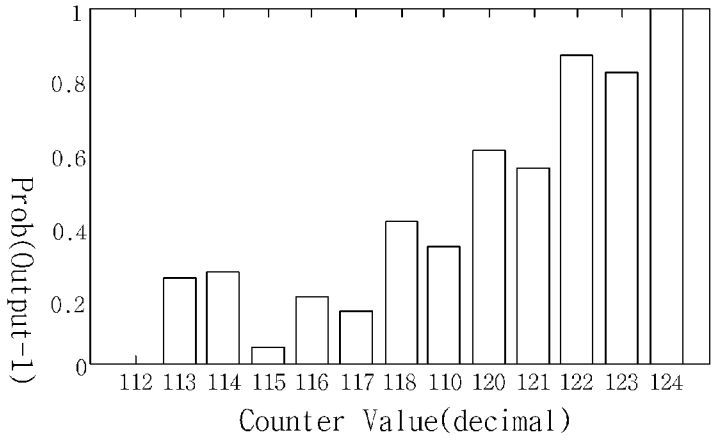
[Fig. 9]


Output control
Delay control
I1
I2
I3
111-1
111-2
111-3
SRAM values
111-6
111
111-4
0
Output

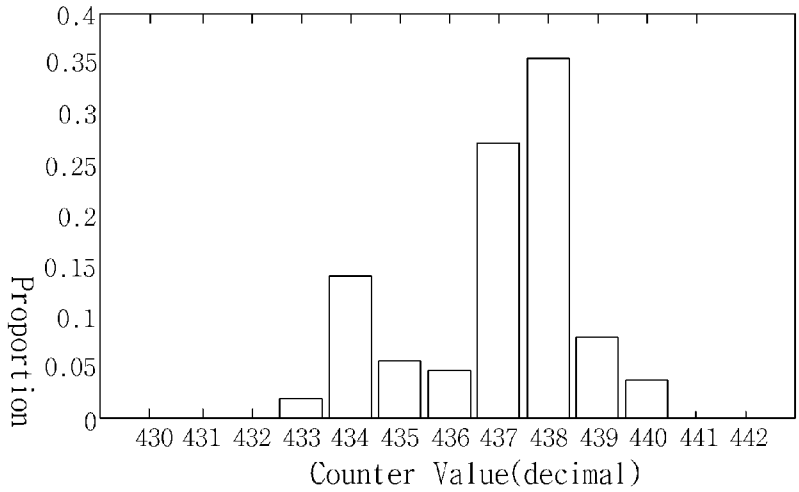
[Fig. 10a]


Prob(Output-1)
Counter Value(decimal)
0
0.2
0.4
0.6
0.8
1
430 431 432 433 434 435 436 437 438 439 440 441 442

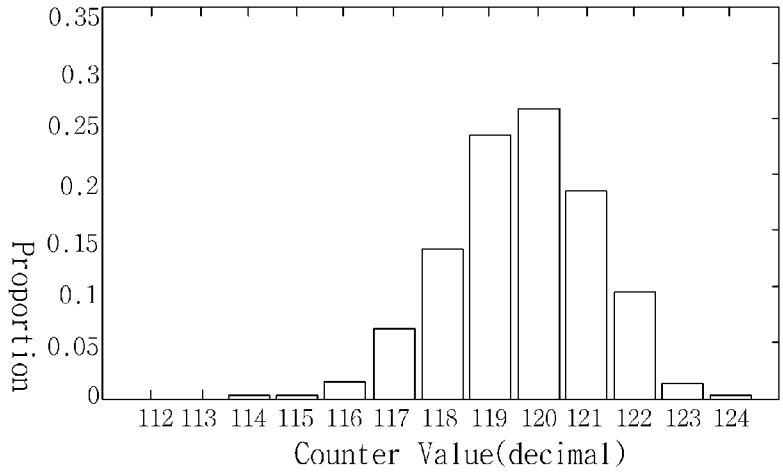
[Fig. 10b]



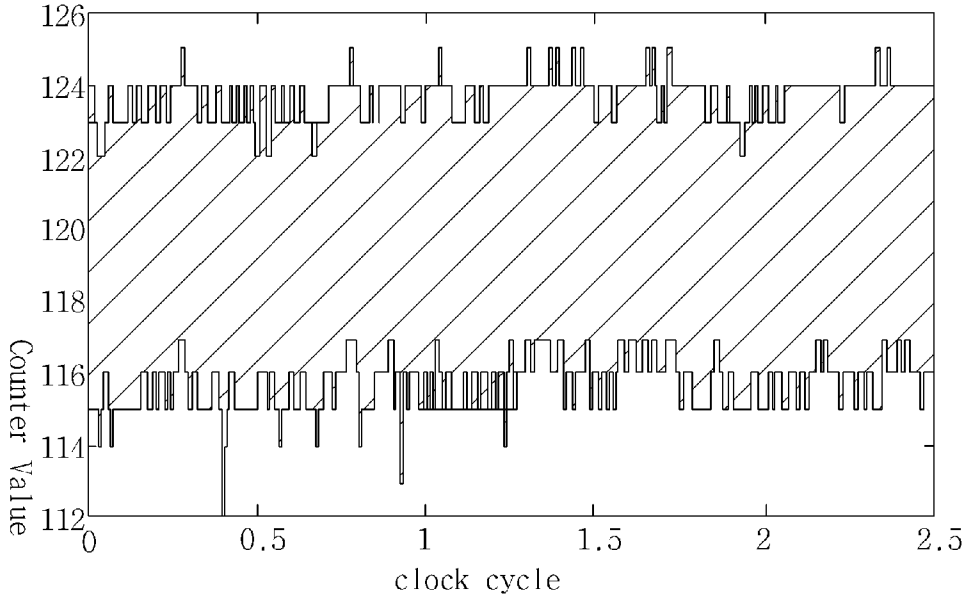
[Fig. 11a]



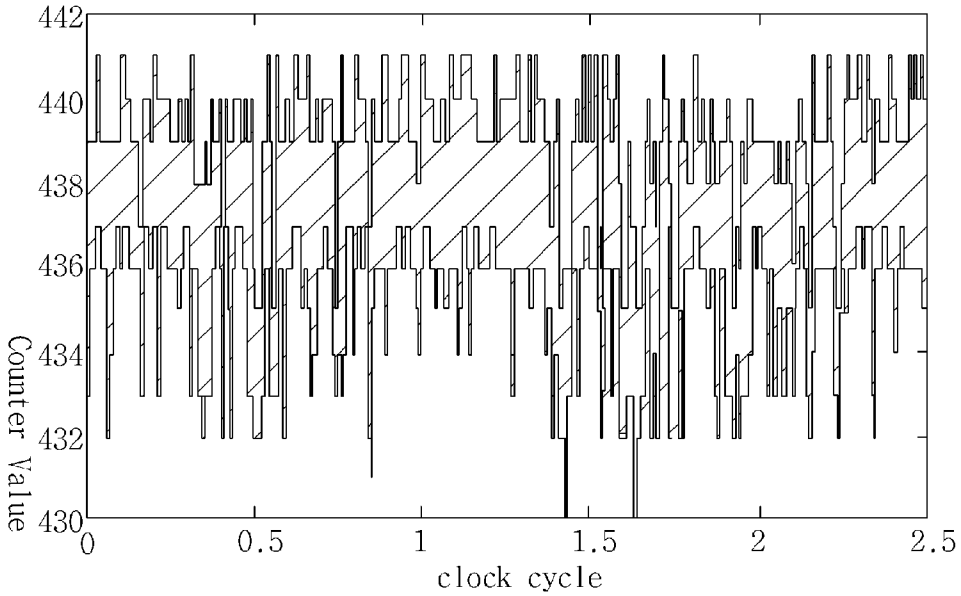
[Fig. 11b]



[Fig. 12a]



[Fig. 12b]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2013/006008

A. CLASSIFICATION OF SUBJECT MATTER

G06F 7/58(2006.01)i, H03K 19/173(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F 7/58; G06F 1/02; H03K 19/173

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean Utility models and applications for Utility models: IPC as above
Japanese Utility models and applications for Utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: FPGA, random number generator

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	KR 10-1127961 B1 (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 12 April 2012	1,2,6,11,16
A	See abstract and paragraphs [0016, 0086], claims 1-3, figures 1-9	3-5,7-10,12-15
A	US 8131789 B2 (VERGNES, Alain et al.) 06 March 2012 See abstract and claims 1-22, figures 1-15	1-16
A	US 2010-0281088 A1 (WILBER, Scott A.) 04 November 2010 See abstract and claims 1-12, figures 1-9	1-16
A	US 8166086 B2 (CHIGO, Giovanni et al.) 24 April 2012 See abstract and claims 1-11, figures 1-4	1-16

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
31 OCTOBER 2013 (31.10.2013)	**31 OCTOBER 2013 (31.10.2013)**
Name and mailing address of the ISA/KR Korean Intellectual Property Office Government Complex-Daejeon, 189 Seonsa-ro, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2013/006008

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-1127961 B1	12/04/2012	NONE	
US 8131789 B2	06/03/2012	US 2009-248771 A1	01/10/2009
US 2010-0281088 A1	04/11/2010	NONE	
US 8166086 B2	24/04/2012	AT 371212 T	15/09/2007
		DE 602004008516 D1	04/10/2007
		DE 602004008516 T2	15/05/2008
		EP 1719052 A1	08/11/2006
		EP 1719052 B1	22/08/2007
		ES 2295829 T3	16/04/2008
		IL 177160A	28/02/2011
		IL 177160D0	20/01/2008
		US 2007-0140485 A1	21/06/2007
		WO 2005-083561 A1	09/09/2005

국제조사보고서

국제출원번호
PCT/KR2013/006008

A. 발명이 속하는 기술분류(국제특허분류(IPC))

G06F 7/58(2006.01)i, H03K 19/173(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)
G06F 7/58; G06F 1/02; H03K 19/173

조사된 기술분야에 속하는 최소문헌 이외의 문헌
한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC
일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))
eKOMPASS(특허청 내부 검색시스템) & 키워드: FPGA,난수발생기

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
X	KR 10-1127961 B1 (한국전자통신연구원) 2012.04.12 요약 및 [0016, 0086] 문단, 청구항 1-3, 도면 1-9 참조	1,2,6,11,16
A		3-5,7-10,12-15
A	US 8131789 B2 (VERGNES ALAIN 외 2명) 2012.03.06 요약 및 청구항 1-22항, 도면 1-15 참조	1-16
A	US 2010-0281088 A1 (WILBER SCOTT A.) 2010.11.04 요약 및 청구항 1-12항, 도면 1-9 참조	1-16
A	US 8166086 B2 (GHIGO GIOVANNI 외 2명) 2012.04.24 요약 및 청구항 1-11, 도면 1-4 참조	1-16

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

"A" 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

"E" 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

"L" 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

"O" 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

"T" 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

"X" 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

"Y" 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2013년 10월 31일 (31.10.2013)	2013년 10월 31일 (31.10.2013)

ISA/KR의 명칭 및 우편주소
대한민국 특허청
(302-701) 대전광역시 서구 청사로 189, 4동 (둔산동, 정부대전청사)
팩스 번호 +82-42-472-7140

심사관
지정훈
전화번호 +82-42-481-5688

국제조사보고서
대응특허에 관한 정보

국제출원번호
PCT/KR2013/006008

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-1127961 B1	2012/04/12	없음	
US 8131789 B2	2012/03/06	US 2009-248771 A1	2009/10/01
US 2010-0281088 A1	2010/11/04	없음	
US 8166086 B2	2012/04/24	AT 371212 T	2007/09/15
		DE 602004008516 D1	2007/10/04
		DE 602004008516 T2	2008/05/15
		EP 1719052 A1	2006/11/08
		EP 1719052 B1	2007/08/22
		ES 2295829 T3	2008/04/16
		IL 177160A	2011/02/28
		IL 177160D0	2008/01/20
		US 2007-0140485 A1	2007/06/21
		WO 2005-083561 A1	2005/09/09