(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2014 년 4 월 17 일 (17.04.2014)

WIPO | PCT

(10) 국제공개번호
WO 2014/058150 A1

(51) 국제특허분류:
G06F 7/58 (2006.01) *G01J 1/02* (2006.01)

(21) 국제출원번호: PCT/KR2013/007510

(22) 국제출원일: 2013 년 8 월 21 일 (21.08.2013)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2012-0111521 2012 년 10 월 8 일 (08.10.2012) KR

(71) 출원인: **에스케이텔레콤 주식회사 (SK TELECOM CO., LTD.)** [KR/KR]; 100-999 서울시 중구 을지로 2 가 11 번지, Seoul (KR).

(72) 발명자: **최정운 (CHOI, Jeong-woon)**; 448-160 경기도 용인시 수지구 죽전동 832 번지 벽산 1 단지아파트 103 동 903 호, Gyeonggi-do (KR). **조정식 (CHO, Jeong-sik)**; 305-333 대전시 유성구 어은동 한빛아파트 108 동 1004 호, Daejeon (KR). **조석범 (CHO, Seok-beom)**; 463-070 경기도 성남시 분당구 야탑동 대진빌라 805 동 304 호, Gyeonggi-do (KR). **박철우 (PARK, Chul-woo)**; 131-140 서울시 중랑구 묵동 13 신내아파트 407 동 1113 호, Seoul (KR).

(74) 대리인: **이철희 (LEE, Chulhee)**; 135-911 서울시 강남구 역삼동 647-13 동궁빌딩 5 층, Seoul (KR).

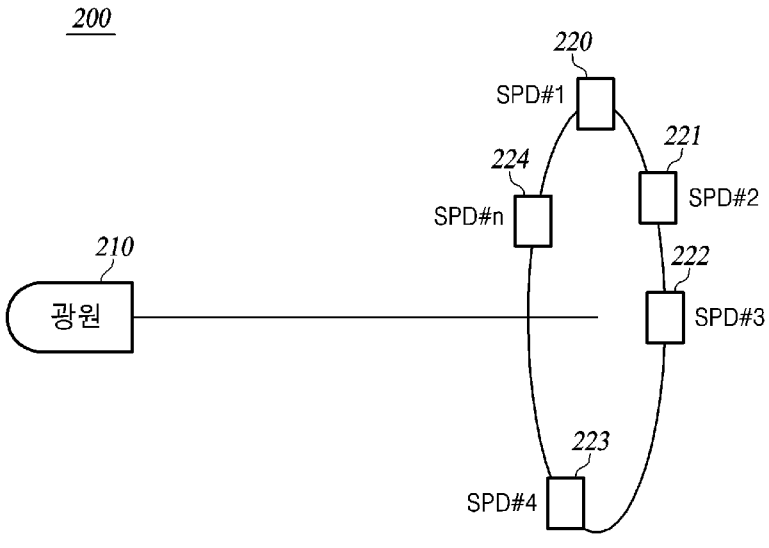
(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, 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, SA, 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))

(54) Title: RANDOM NUMBER GENERATING METHOD AND APPARATUS USING LIGHT SOURCE AND SINGLE PHOTON DETECTOR

(54) 발명의 명칭 : 광원과 단일광자검출기를 이용한 난수 생성 방법 및 장치



210 ... Light source

(57) Abstract: The present invention relates to a random number generating method and apparatus using a light source and a single photon detector. According to an aspect of this embodiment, there is provided the random number generating apparatus that generates a random number and includes: a light source that emits luminous flux, the light intensity distribution of which is symmetrical with respect to a central axis; and a plurality of single photon detectors that are positioned radially apart from each other from an extending line of the central axis of the light source to generate a bit value of either 0 or 1 depending on whether a photon is detected or not.

(57) 요약서: 광원과 단일광자검출기를 이용한 난수 생성 방법 및 장치를 개시한다. 본 실시예의 일 측면에 의하면, 난수를 생성하는 난수 생성장치에 있어서, 광세기(Light Intensity) 분포가 중심축에 대칭적인 광속(Luminous Flux)을 출사하는 광원 및 상기 광원의 중심축의 연장선으로부터 방사상으로 이격되어 위치하여, 광자의 검출 여부에 따라 0 또는 1 중 어느 하나의 비트값을 생성하는 복수의 단일광자검출기를 포함하는 난수 생성장치를 제공한다.

WO 2014/058150 A1

명세서

발명의 명칭: 광원과 단일광자검출기를 이용한 난수 생성 방법 및 장치

기술분야

[1] 본 실시예는 광원과 단일광자검출기를 이용한 난수 생성 방법 및 장치에 관한 것이다. 더욱 상세하게는, 광원이 갖는 통계적인 성질과 단일광자 검출기가 갖는 검출효율을 활용하여 진난수를 생성하는, 광원과 단일광자검출기를 이용한 난수 생성 방법 및 장치에 관한 것이다.

배경기술

[2] 이 부분에 기술된 내용은 단순히 본 실시예에 대한 배경 정보를 제공할 뿐 종래기술을 구성하는 것은 아니다.

[3] 수치 시뮬레이션, 통계분석으로부터 암호화에 이르기까지 다양한 응용분야에서 난수성(Randomness)을 필요로 한다. 난수성을 얻기 위한 방법은 의사 난수(Pseudo Random Number)를 생성하는 간단한 수학적인 기법에서 진난수(True Random Number)를 생성하는 물리적인 현상을 이용하는 방법으로 발전해왔다.

[4] TRNG(True Random Number Generator)는 저항 소자, 반도체 다이오드, 방사능물질로부터의 전기적인 잡음 등에 기초하여 진난수를 생성하는 장치로서, 의사난수를 생성하는 PRNG(Pseudo Random Number Generator)와 상대되는 개념의 장치를 이른다.

[5] TRNG 중의 하나인 QRNG(Quantum Random Number Generator)는 진난수를 생성하기 위해 양자 역학적 원리를 활용하여 TRNG를 구현한다. 빛의 양자성에 기초한 여러가지 QRNG가 제안되었는데, 대부분의 시스템들은 데이터를 생성하기 위해 광분할기(Beam Splitter)에 입사되는 광자의 거동에 의존한다.

[6] 도 1은 광분할기에 입사되는 광자의 거동을 이용한 종래의 양자난수생성기(QRNG)의 예시도이다.

[7] 도 1에 도시된 바와 같이, 광원(110)으로부터 입사된 광자(120)는 광분할기(130)에 의해 두 개의 경로 중 하나를 따라 진행하다가 대응되는 단일광자검출기(Single Photon Detector: SPD; 140, 141)에 의해 검출된다. 어느 단일광자검출기(140, 141)가 입사 광자(120)를 검출하느냐에 따라 0 또는 1이 생성된다. 이러한 방법은 각 광자(120)마다 기껏해야 하나의 비트만을 생성할 수 있다는 결점을 가지며, 실제 구현시에는 이보다 훨씬 적은 비트가 생성된다. 즉, 비트 생성에 기여하는 것은 탐지이벤트이므로, 비트 생성률은 검출 속도와 검출 효율에 의해 제한을 받게 되고, 따라서 랜덤 비트를 생성하는 속도는 단일광자검출기(140, 141)의 최고 검출속도보다 상당히 낮을 수밖에 없다. 이러한 문제를 보완하기 위해 복수의 단일광자검출기로 QRNG를 구현하는

방법이 제안되었으나, 각 단일광자검출기의 서로 다른 검출 효율에 의해 편향(Bias)이 생기는 문제를 안고 있다.

발명의 상세한 설명

기술적 과제

[8] 전술한 문제점을 해결하기 위해 본 실시예는, 빛이 갖는 통계적 성질과 단일광자검출기의 검출효율을 이용하되, 복수의 단일광자검출기를 통해 난수 생성속도를 높일 수 있는 난수 생성 장치 및 방법을 제공하는 데 주된 목적이 있다.

과제 해결 수단

[9] 본 실시예의 일 측면에 의하면, 난수를 생성하는 난수 생성장치에 있어서, 광세기 분포(Light Intensity)가 중심축에 대칭적인 광속(Luminous Flux)을 출사하는 광원 및 상기 광원의 중심축의 연장선으로부터 방사상으로 이격되어 위치하여, 광자의 검출 여부에 따라 0 또는 1 중 어느 하나의 비트값을 생성하는 복수의 단일광자검출기를 포함하는 난수 생성장치를 제공한다.

[10] 상기 광원의 상기 광세기 분포는 가우시안 분포(Gaussian Distribution)를 포함하는 선대칭 분포(Axisymmetric Distribution)를 따르는 것이 바람직하다.

[11] 또한, 상기 광원은 발광소자의 광속을 필터링하여 중심축에 대칭적인 광속을 생성하는 광학 수단을 이용한 것일 수 있다.

[12] 또한, 상기 단일광자검출기의 광자검출확률은, $P = 1 - e^{-\eta\mu} + \delta$으로 표현될 수 있다. 여기서 P는 단일광자검출기의 광자검출확률, η는 단일광자검출기의 광자검출효율, μ는 단일광자검출기에 입사되는 광속의 세기, δ는 단일광자검출기의 암계수발생확률(Dark Count Probability)을 고려하기 위한 계수이다.

[13] 또한, 상기 η, μ 및 δ 값은 상기 단일광자검출기의 광자검출확률 P가 0.5가 되도록 설정되는 것이 바람직하다.

[14] 또한, 상기 복수의 단일광자검출기는 상기 광원의 중심축의 연장선으로부터 방사상으로 동일거리만큼 이격되어 위치하는 것이 바람직하다.

[15] 또한, 상기 난수 생성장치는 상기 복수의 단일광자검출기로부터 출력되는 비트들을 기초로 상기 난수를 생성하는 난수 생성부를 더 포함할 수 있다.

[16] 또한, 상기 난수 생성부는 각 클럭마다 상기 복수의 단일광자검출기로부터 출력되는 비트의 집합을 순차적으로 배열하여 상기 난수를 생성할 수 있다.

[17] 또한, 상기 난수 생성부는 상기 복수의 단일광자검출기로부터 출력되는 비트들에 관하여 패리티 생성 연산을 수행하여 상기 난수를 생성할 수 있다.

[18] 또한, 상기 난수 생성부는 상기 복수의 단일광자검출기로부터 동일한 클럭에

출력되는 비트의 집합을 클럭 순서에 따라 순차적으로 배열하여 초기 비트열(Raw Bit String)을 생성하고, 생성된 상기 초기 비트열을 기초로 패리티 생성 연산을 수행함으로써 상기 난수를 생성할 수 있다.

[19] 또한, 상기 난수 생성부는 생성된 상기 초기 비트열에 대해 일정 크기의 마스크(Mask)를 적용하여 패리티 비트를 생성하되, 상기 마스크를 현재 패리티 비트를 생성한 위치로부터 적어도 1비트 이동하여 다음 패리티 비트를 생성하는 방식으로 연산함으로써 상기 난수를 생성할 수 있다.

[20] 더불어, 상기 난수 생성부는 상기 복수의 단일광자검출기로부터 출력되는 비트열 각각에 대해 패리티 생성 연산을 수행한 후, 각 단일광자검출기마다 생성된 패리티 비트를 순차적으로 배열함으로써, 상기 난수를 생성할 수 있다.

[21] 본 실시예의 다른 측면에 의하면, 중앙을 기준으로 대칭적인 광세기 분포를 갖는 광속을 출사하는 과정, 상기 광세기 분포의 대칭축으로부터 방사상으로 이격되어 위치한 복수의 단일광자검출기의 광자 검출 여부에 따라 비트열을 생성하는 과정 및 상기 복수의 단일광자검출기로부터 출력되는 비트열을 기초로 난수를 생성하는 후처리 과정을 포함하는 광원 및 단일광자검출기를 이용한 난수 생성 방법을 제공한다.

[22] 본 실시예의 또다른 측면에 의하면, 난수를 생성하는 장치에 있어서, 광원으로부터 출사된 광속으로부터 광자를 복수의 지점에서 검출하고, 상기 광자의 검출 여부를 0 또는 1의 디지털값으로 변환한 후 상기 디지털값에 수학적 연산을 취한 결과로써 난수를 생성하는 장치를 제공한다.

[23] 본 실시예의 또다른 측면에 의하면, 난수를 생성하는 방법에 있어서 광원으로부터 출사된 광속으로부터 광자를 복수의 지점에서 검출하고, 상기 광자의 검출 여부를 0 또는 1의 디지털값으로 변환한 후 상기 디지털값에 수학적 연산을 취한 결과로써 난수를 생성하는 방법을 제공한다.

발명의 효과

[24] 이상에서 설명한 바와 같이 본 실시예에 의하면, N개의 단일광자검출기를 통해 클럭마다 N개의 비트를 생성함으로써, 다른 단일광자검출기 기반의 진난수 생성 방법보다 빠른 속도로 난수를 생성할 수 있다.

[25] 또한, 단일광자검출기의 광자검출효율, 단일광자검출기에 입사되는 광속의 광도 등을 조절하여 각각의 단일광자검출기의 광자검출확률을 0.5로 설정할 수 있으므로, 코히런트 광펄스(Coherent Light Pulse)를 생성하는 레이저 다이오드(Laser Diode)뿐만 아니라, 저가형의 LED를 광원으로 사용하는 것이 가능하며, 실제적으로 임의의 광원을 사용하는 것도 무방하다.

[26] 또한, 복수의 단일광자검출기의 성능 편차 등으로 인하여 난수열에 포함될 수 있는 편향(Bias)를 제거하기 위해 패리티 연산을 수행함으로써 난수성을 높일 수 있다.

[27] 더불어, 본 실시예에 따른 난수 생성장치는 진난수를 생성할 수 있으며, 따라서

양자 암호(Quantum Cryptography) 분야에 적용하기 적합하다.

도면의 간단한 설명

[28] 도 1은 광분할기에 입사되는 광자의 거동을 이용한 종래의 양자난수생성기(QRNG)의 예시도이다.

[29] 도 2는 본 발명의 일 실시예에 따른 난수 생성장치의 구성을 개략적으로 도시한 도면이다.

[30] 도 3은 광원으로부터 발생되는 광속의 광세기 분포를 예시한 도면이다.

[31] 도 4a 및 도 4b는 각 단일광자검출기가 각 클럭마다 출력하는 비트를 순차적으로 배열하여 난수열을 생성하는 방법을 예시한 도면이다.

[32] 도 5a, 도 5b 및 도 5c는 단위 비트열을 순차적으로 배열하여 생성한 초기 비트열에 대해 배타적 논리합 연산을 수행하여 난수열을 생성하는 방법을 예시한 도면이다.

[33] 도 6은 각 단일광자검출기의 단위 비트열에 대해 배타적 논리합 연산을 수행하여 생성한 뒤 그 결과를 순차적으로 배열하여 난수열을 생성하는 방법을 예시한 도면이다.

발명의 실시를 위한 형태

[34] 이하, 본 발명의 일부 실시예들을 예시적인 도면을 통해 상세하게 설명한다. 각 도면의 구성요소들에 참조부호를 부가함에 있어서, 동일한 구성요소들에 대해서는 비록 다른 도면상에 표시되더라도 가능한 한 동일한 부호를 가지도록 하고 있음에 유의해야 한다. 또한, 본 발명을 설명함에 있어, 관련된 공지 구성 또는 기능에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명은 생략한다.

[35] 또한, 본 발명의 구성 요소를 설명하는 데 있어서, 제 1, 제 2, A, B, (a), (b) 등의 용어를 사용할 수 있다. 이러한 용어는 그 구성 요소를 다른 구성 요소와 구별하기 위한 것일 뿐, 그 용어에 의해 해당 구성 요소의 본질이나 차례 또는 순서 등이 한정되지 않는다.

[36] 도 2는 본 발명의 일 실시예에 따른 난수 생성장치의 구성을 개략적으로 도시한 도면이다.

[37] 도 2에 도시된 바와 같이, 본 실시예에서 난수 생성장치(200)는 광세기(Light Intensity) 분포가 광원의 중심축에 대칭적인 광속(Luminous Flux)을 출사하는 광원(210) 및 광원(210)의 중심축의 연장선으로부터 방사상으로 동일한 거리에 위치하는 N개의 단일광자검출기(Single Photon Detector: SPD; 220~224)를 포함한다. 각각의 단일광자검출기(220~224)는 각 클럭마다 광자의 검출 여부에 따라 0 또는 1의 비트값을 생성한다. N개의 단일광자검출기(220~224)로부터 각 클럭마다 1개의 비트가 생성되므로, 난수 생성장치(200)는 클럭당 N개의 비트를 얻을 수 있다. 결과적으로, 도 1에 예시된 바와 같은 종래의 단일광자검출기 기반의 QRNG 장치보다 N배 빠른 비트열 생성 속도를 갖게 된다. 또한 도 2에

도시하지는 않았지만, 난수 생성장치(200)는 N개의 단일광자검출기로부터 출력되는 비트들을 기초로 난수열을 생성하는 난수 생성부를 더 포함할 수 있다. 난수 생성부가 난수를 생성하는 방법은 도 4a 내지 도 6을 참조하여 별도로 설명하기로 한다.

[38] 각 단일광자검출기(220~224)의 출력 비트를 기초로 난수를 생성하기 위해서는 각 단일광자검출기가 비트 0 또는 1을 동일한 비율로 출력하는 것이 바람직한데, 이는 각 단일광자검출기(220~224)의 광자 검출확률이 50%로 제어되어야 함을 의미한다. 이하에서는 각 단일광자검출기(220~224)의 광자 검출확률에 관하여 기술한다.

[39] 단일광자검출기에는 아발란치 광다이오드(Avalanche Photodiode)로 불리는 반도체 광검출기(SAPD)와 음극과 양극 사이에 증폭판을 넣어서 작동시키는 광증폭관(PMT)검출기 등이 있다.

[40] 보통 미약한 레이저 펄스들의 광자 수 분포는 푸아송 분포(Poisson Distribution)을 갖는다. 부분적으로 흡수된 빛의 광자 수 분포는 초기 필드의 베르누이 변환(Bernoulli Transform)을 따르기 때문에, 미약한 레이저 펄스들의 탐지된 광자 수 분포는 다음의 수학식 1을 따른다.

[41] 수학식 1

$$P\eta(n)=\frac{(\eta\lambda)^{n}e^{-\eta\lambda}}{n!}$$

[42] 여기서,

P_{η}

는 탐지된 광자 수 분포확률,

λ

는 미약한 레이저 펄스들의 평균 광자 수,

η

는 단일광자검출기의 탐지 효율을 의미한다.

[43] 일반적인 단일광자검출기는 광자의 탐지/비탐지만을 확인할 수 있을 뿐, 탐지된 광자의 수를 구별하는 것이 곤란하다. 이로 인해 단일광자검출기로부터, 광자가 탐지되지 않을 때 0을 얻을 수 있고, 하나 이상의 광자가 탐지된 때 1을 얻을 수 있다.

[44] 따라서 0과 1의 결과를 얻을 수 있는 확률은 각각 수학식 2와 수학식 3으로 표현될 수 있다.

[45] 수학식 2

$$P\eta(0) = e^{-\eta\lambda}$$

[46] 수학식 3

$$P\eta(n\geq 1) = 1 - e^{-\eta\lambda}$$

[47] 수학식 2 및 수학식 3으로부터

$$\eta\lambda = 0.693$$

일 때

$$P\eta(0) = 0.5, \quad P\eta(n\geq 1) = 0.5$$

를 얻을 수 있음을 알 수 있다.

[48] 한편, 단일광자검출기는 광원으로부터 입사되는 광자가 없는 경우에도 광자가 탐지되었을 때와 동일한 신호를 출력하는 경우가 발생하는데, 이러한 탐지비율을 암계수 발생확률(Dark Count Probability)이라고 한다. 암계수로 표현되는 아발란치 광다이오드의 암전류의 발생요인은 크게 세 가지로 구분할 수 있는데, 첫째는 열적 여기에 의한 전자-홀 쌍의 생성, 둘째는 공핍 영역에서 터널효과로 인한 전류 발생, 셋째는 이전에 들어온 빛에 의해 생성된 전하가 갇혀 있다가 다음 번 역바이어스에 의해 아발란치 되는 현상(Afterpulsing)이다. 이러한 암계수 발생을 고려하여 단일광자검출기의 광자 검출확률을 표현하면 수학식 4와 같다.

[49] 수학식 4

$$P = 1 - e^{-\eta\mu} + \delta$$

[50] 여기서,

P

는 단일광자검출기의 광자 검출확률,

η

는 단일광자검출기의 검출효율,

μ

는 단일광자검출기에 입사되는 광속(Luminous Flux)의 광세기,

δ

는 온도, 잡음 등에 따른 단일광자검출기의 암계수 발생확률을 고려하기 위한 계수이다.

[51] η

은 구현시 사용되는 단일광자검출기의 정해진 특성이고,

δ

은 제어하기 곤란한 변수이므로,

μ

를 조절함으로써 단일광자검출기의 광자 검출확률

P

를 0.5로 설정할 수 있다. 예를 들어,

$$\eta = 0.1,\ \delta = 1\times10^{-5}$$

라면, 단일광자검출기에 입사되는 광속의 광세기

μ

를 7로 조절함으로써 광자 검출확률

P

를 0.5로 설정할 수 있다.

μ

는 광원의 출력을 조절하거나 단일광자검출기의 광원까지의 이격거리나 광원의 중심축으로부터의 이격 거리 등을 조절함으로써 제어될 수 있다.

[52] 도 3은 광원으로부터 발생되는 광속의 광세기 분포를 예시한 도면이다.

[53] 본 실시예에 따른 난수 생성 장치는 복수의 단일광자검출기를 사용하므로, 각 단일광자검출기에 입사되는 광속(Luminous Flux)의 광세기

μ

가 동일하게 제어되는 것이 바람직하다.

[54] 만일 광원으로부터 출사되는 광속의 광세기 분포가 선대칭 분포(Axisymmetric Distribution)를 갖는다면, 복수의 단일광자검출기를 광원의 중심축의 연장선으로부터 방사상으로 동일한 거리에 위치시킴으로써 각 단일광자검출기에 입사되는 광속의 광세기를 동일하게 할 수 있다. 예컨대 도 3에 도시된 바와 같이, 가우시안 분포(Gaussian Distribution)를 갖는 광속을 출사하는 광원을 사용하는 경우 광원(210)의 중심축의 연장선으로부터 방사상으로 동일한 거리만큼 떨어져 위치하는 N개의 단일광자검출기(220~224)에는 동일한 세기의 광속이 입사하게 된다. 따라서 본 실시예에 사용되는 광원은 중심축에 대칭적인 광세기 분포를 갖는 광속을 출사하는 광원인 것이 바람직하다.

[55] 한편, 도 1에 예시된 종래의 양자난수 생성 장치가 광분할기에 입사되는 광자의 거동에 의존하는 것과는 달리, 본 실시예에서는 단일광자검출기의 광자검출 효율 또는 검출확률을 이용하므로, 코히런트 광펄스(Coherent Light Pulse)를 생성하는 레이저 다이오드(Laser Diode)뿐만 아니라, 저가형의 LED를 광원으로

사용하는 것이 가능하며, 실제적으로 임의의 광원을 사용하는 것도 무방하다. 그러나 이러한 광원에 포함된 발광소자들은 대개 광세기 분포가 가우시안 분포 내지는 선대칭 분포를 따르지 않으므로, 이러한 경우에는 공간필터(Spatial Filter), 렌즈 등의 광학 수단을 이용하여 임의의 선대칭 분포를 갖도록 할 수 있다.

[56] 이하에서는 도 2의 복수의 단일광자검출기(220~224)에서 생성되는 비트열로부터 난수열을 생성하는 방법을 도 4a 내지 도 6을 참조하여 설명하기로 한다.

[57] 앞서 언급한 바와 같이, 각 단일광자검출기(220~224)는 각 클럭마다 광자의 검출여부에 따라 0 또는 1 값을 갖는 비트를 출력하는데, 이하에서는 1개의 단일광자검출기(220~224)가 출력하는 비트들의 집합을 '단위 비트열'이라고 칭하기로 한다.

[58] 도 4a 및 도 4b는 각 단일광자검출기가 각 클럭마다 출력하는 비트를 순차적으로 배열하여 난수열을 생성하는 방법을 예시한 도면이다.

[59] 도 4a 및 도 4b와 같이 5개의 단일광자검출기(410)를 이용하여 난수 생성장치를 구현한 경우를 가정하면, 난수 생성부(420)는 각 클럭마다 5개의 단일광자검출기(410)에서 출력된 비트의 집합인 {a1, b1, c1, d1, e1}, {a2, b2, c2, d2, e2}, {a3, b3, c3, d3, e3}...을 순차적으로 배열함으로써, [a1, b1, c1, d1, e1, a2, b2, c2, d2, e2, a3, b3, c3, d3, e3...]형태의 초기 비트열(Raw Bit String)을 난수열로 출력할 수 있다.

[60] 각 단일광자검출기(410)의 광자 검출확률이 정확히 0.5라면, 각 단일광자검출기(410)가 출력하는 단위 비트열은 완전한 난수성을 갖게 되고, 이와 같은 순차적 배열만으로도 편향(Bias)없는 난수열을 얻을 수 있다.

[61] 그러나 실제적인 측면에서 각 단일광자검출기(410)의 성능(예컨대 η, δ) 등으로 인해 각 단일광자검출기가 출력하는 비트열에는 일정 비율의 편향이 존재할 수 있다. 따라서 도 4a 및 도 4b에 예시된 것처럼 각 단위 비트열을 순차적으로 배열하여 곧바로 난수열을 생성하는 것보다는 후처리 연산을 통해 난수성(Randomness)을 높일 필요가 있다.

[62] 난수성을 높이기 위한 후처리 연산에는 다양한 방법이 있을 수 있으나, 여기서는 패리티 비트 연산을 기초로 한 후처리 연산 방법을 예시적으로 설명하기로 한다.

[63] 도 5a 내지 도 5c는 단위 비트열을 순차적으로 배열하여 생성한 초기 비트열에 대해 배타적 논리합 연산을 수행하여 난수열을 생성하는 방법을 예시한

도면이다.

[64] 도 5a에 도시된 바와 같이, 난수 생성부(520)는 각 단일광자검출기(510)가 각 클럭마다 출력하는 비트를 순차적으로 배열하여 초기 비트열을 생성하고, 생성된 초기 비트열에 대해 배타적 논리합(Exclusive-OR) 연산, 즉 패리티 비트(Parity Bit)를 생성하는 연산을 수행함으로써 생성된 랜덤 비트열(Random Bit String)을 난수열로서 출력할 수 있다. 여기서, 난수 생성부의 구성 521 및 522는 반드시 물리적으로 구분되는 구성이라기보다는 수행하는 기능을 기준으로 논리적으로 구분한 것에 불과하다. 초기 비트열로부터 배타적 논리합 연산을 수행하는 방법은 도 5b 및 도 5c와 같이 2가지 방법이 있을 수 있다.

[65] 첫 번째 방법은 초기 비트열을 일정 개수의 비트구간으로 나누어 패리티 비트를 생성하는 방법으로, 도 5b에서 5개의 비트마다 패리티 비트를 생성하는 방법을 예시하였다. 이러한 패리티 비트 생성 방법에서는, 패리티 비트를 생성하는 구간의 크기를 크게 할수록 초기 비트열이 갖는 편향을 더 많이 제거하게 되고, 결과적으로 랜덤 비트열의 난수성을 증가시킨다. 반면, 패리티 비트를 생성하는 구간의 크기가 증가함에 따라 랜덤 비트열의 생성률은 감소하게 되는데, 도 5b으로부터 5개의 비트마다 배타적 논리합 연산을 수행하는 경우에 얻을 수 있는 랜덤 비트열의 데이터량은 초기 비트열의 1/5에 불과함을 알 수 있다.

[66] 두 번째 방법은 첫 번째 방법의 랜덤 비트열의 생성률 감소 문제를 피할 수 있는 방법으로, 일정 크기의 마스크(Mask)를 적용하여 패리티 비트를 생성하되, 상기 마스크를 1 비트씩 이동하면서 다음 패리티 비트를 연산하는 방법이다. 예컨대 도 5c에 예시된 바와 같이, 5개의 비트들에 대해 패리티 비트를 생성하는 경우, 첫 패리티 비트를 {a1, b1, c1, d1, e1} 조합으로부터 연산하고, 두 번째 패리티 비트는 1비트 이동하여 {b1, c1, d1, e1, a2} 조합으로부터 연산한다.

[67] 한편, 도 5a 내지 도 5c에서 예시한 배타적 논리합 연산은 초기 비트열에 대해 적용함으로써 난수성을 증가시켰으나, 이와 달리 초기 비트열을 생성하기에 앞서 단일광자검출기의 출력인 단위 비트열 각각에 대해 배타적 논리합 연산을 수행할 수도 있다. 이를 도 6을 참조하여 설명하기로 한다.

[68] 도 6은 각 단일광자검출기의 단위 비트열에 대해 배타적 논리합 연산을 수행하여 생성한 뒤 그 결과를 순차적으로 배열하여 난수열을 생성하는 방법을 예시한 도면이다.

[69] 도 6에 예시된 바와 같이, 난수 생성부(620)는 각 단일광자 검출기(610)가 출력하는 비트들, 즉 단위 비트열에 대해 각각 배타적 논리합 연산을 수행할 수 있다. 이때 배타적 논리합 연산을 수행하는 방법은 도 5b 또는 도 5c에서 설명한 방식과 동일한 방식이 적용될 수 있다. 도 6에서 각 단위 비트열에 수행한 배타적 논리합 연산의 결과를 '단위 랜덤 비트열(Unit Random Bit String)'로 표시하였다. 그 후 난수 생성부(620)는 도 4b에서 설명한 방식과 동일한 방식으로 각 단위 랜덤 비트열에 포함된 패리티 비트를 순차적으로 나열함으로써, 난수열로

사용될 수 있는 랜덤 비트열을 생성할 수 있다. 여기서, 난수 생성부의 구성 621 및 622는 반드시 물리적으로 구분되는 구성이라기보다는 수행하는 기능을 기준으로 논리적으로 구분한 것에 불과하다.

[70] 이상의 설명은 본 실시예의 기술 사상을 예시적으로 설명한 것에 불과한 것으로서, 본 실시예가 속하는 기술 분야에서 통상의 지식을 가진 자라면 본 실시예의 본질적인 특성에서 벗어나지 않는 범위에서 다양한 수정 및 변형이 가능할 것이다. 따라서, 본 실시예들은 본 실시예의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시예에 의하여 본 실시예의 기술 사상의 범위가 한정되는 것은 아니다. 본 실시예의 보호 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 실시예의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

[71]

[72] CROSS-REFERENCE TO RELATED APPLICATION

[73] 본 특허출원은 2012년 10월 08일 한국에 출원한 특허출원번호 제 10-2012-0111521 호에 대해 미국 특허법 119(a)조(35 U.S.C § 119(a))에 따라 우선권을 주장하면, 그 모든 내용은 참고문헌으로 본 특허출원에 병합된다. 아울러, 본 특허출원은 미국 이외에 국가에 대해서도 위와 동일한 이유로 우선권을 주장하면 그 모든 내용은 참고문헌으로 본 특허출원에 병합된다.

청구범위

[청구항 1] 난수(Random Number)를 생성하는 난수 생성 장치(Random Number Generator)에 있어서,
광세기(Light Intensity) 분포가 중심축에 대칭적인 광속(Luminous Flux)을 출사하는 광원; 및
상기 광원의 중심축의 연장선으로부터 방사상으로 이격되어 위치하여, 광자의 검출 여부에 따라 0 또는 1 중 어느 하나의 비트값을 생성하는 복수의 단일광자검출기(Single Photon Detector: SPD)
를 포함하는 난수 생성 장치.

[청구항 2] 제1항에 있어서,
상기 광원의 상기 광세기 분포는,
가우시안 분포(Gaussian Distribution)를 포함하는 선대칭 분포(Axisymmetric Distribution)를 따르는 것을 특징으로 하는 난수 생성 장치.

[청구항 3] 제1항에 있어서,
상기 광원은,
발광소자의 광속을 필터링하여 중심축에 대칭적인 광속을 생성하는 광학 수단을 이용한 것임을 특징으로 하는 난수 생성 장치.

[청구항 4] 제1항에 있어서,
상기 단일광자검출기의 광자검출확률은,
$P = 1 - e^{-\eta\mu} + \delta$으로 표현되되, 여기서 P는 단일광자검출기의 광자검출확률, η는 단일광자검출기의 광자검출효율, μ는 단일광자검출기에 입사되는 광속(Luminous Flux)의 광세기, δ는 단일광자검출기의 암계수발생확률(Dark Count Probability)을 고려하기 위한 계수인 것을 특징으로 하는 난수 생성 장치.

[청구항 5] 제4항에 있어서,
상기 η, μ 및 δ 값은,
상기 단일광자검출기의 광자검출확률 P가 0.5가 되도록 설정된 것을 특징으로 하는 난수 생성 장치.

[청구항 6] 제1항에 있어서,

상기 복수의 단일광자검출기는,
상기 광원의 중심축의 연장선으로부터 방사상으로 동일거리만큼 이격되어 위치한 것을 특징으로 하는 난수 생성 장치.

[청구항 7] 제1항에 있어서,
상기 복수의 단일광자검출기로부터 출력되는 비트들을 기초로 상기 난수를 생성하는 난수 생성부를 더 포함하는 난수 생성 장치.

[청구항 8] 제7항에 있어서,
상기 난수 생성부는,
각 클럭마다 상기 복수의 단일광자검출기로부터 출력되는 비트의 집합을 순차적으로 배열하여 상기 난수를 생성하는 것을 특징으로 하는 난수 생성 장치.

[청구항 9] 제7항에 있어서,
상기 난수 생성부는,
상기 복수의 단일광자검출기로부터 출력되는 비트들에 관하여 패리티 생성 연산을 수행하여 상기 난수를 생성하는 것을 특징으로 하는 난수 생성 장치.

[청구항 10] 제9항에 있어서,
상기 난수 생성부는,
상기 복수의 단일광자검출기로부터 동일한 클럭에 출력되는 비트의 집합을 클럭 순서에 따라 순차적으로 배열하여 초기 비트열(Raw Bit String)을 생성하고, 생성된 상기 초기 비트열을 기초로 패리티 생성 연산을 수행함으로써 상기 난수를 생성하는 것을 특징으로 하는 난수 생성 장치.

[청구항 11] 제10항에 있어서,
상기 난수 생성부는,
생성된 상기 초기 비트열에 대해 일정 크기의 마스크(Mask)를 적용하여 패리티 비트를 생성하되, 상기 마스크를 현재 패리티 비트를 생성한 위치로부터 적어도 1비트 이동하여 다음 패리티 비트를 생성하는 방식으로 연산함으로써 상기 난수를 생성하는 것을 특징으로 하는 난수 생성 장치.

[청구항 12] 제9항에 있어서,
상기 난수 생성부는,
상기 복수의 단일광자검출기로부터 출력되는 비트열 각각에 대해 패리티 생성 연산을 수행한 후, 각 단일광자검출기마다 생성된 패리티 비트를 순차적으로 배열함으로써, 상기 난수를 생성하는 것을 특징으로 하는 난수 생성 장치.

[청구항 13] 중앙을 기준으로 대칭적인 광세기 분포를 갖는 광속을 출사하는 과정;

상기 광세기 분포의 대칭축으로부터 방사상으로 이격되어 위치한 복수의 단일광자검출기의 광자 검출 여부에 따라 비트열을 생성하는 과정; 및

상기 복수의 단일광자검출기로부터 출력되는 비트열을 기초로 난수를 생성하는 후처리 과정

을 포함하는 광원 및 단일광자검출기를 이용한 난수 생성 방법.

[청구항 14] 제13항에 있어서,

상기 대칭적인 광세기 분포는,

가우시안 분포를 포함하는 선대칭 분포를 따르는 것을 특징으로 하는 광원 및 단일광자검출기를 이용한 난수 생성 방법.

[청구항 15] 제13항에 있어서,

상기 단일광자검출기의 광자검출확률은 0.5인 것을 특징으로 하는 광원 및 단일광자검출기를 이용한 난수 생성 방법.

[청구항 16] 제13항에 있어서,

상기 후처리 과정은,

상기 복수의 단일광자검출기로부터 동일한 클럭에 출력되는 비트의 집합을 클럭 순서대로 순차적으로 배열함으로써 상기 난수를 생성하는 것을 특징으로 하는 광원 및 단일광자검출기를 이용한 난수 생성 방법.

[청구항 17] 제16항에 있어서,

상기 후처리 과정은,

상기 복수의 단일광자검출기로부터 동일한 클럭에 출력되는 비트의 집합을 클럭 순서대로 순차적으로 배열하여 초기 비트열을 생성하고, 생성된 상기 초기 비트열을 기초로 패리티 생성 연산을 수행함으로써 상기 난수를 생성하는 것을 특징으로 하는 광원 및 단일광자검출기를 이용한 난수 생성 방법.

[청구항 18] 제17항에 있어서,

상기 후처리 과정은,

생성된 상기 초기 비트열에 대해 일정 길이마다 패리티 비트를 생성함으로써 상기 난수를 생성하는 것을 특징으로 하는 광원 및 단일광자검출기를 이용한 난수 생성 방법.

[청구항 19] 제17항에 있어서,

상기 후처리 과정은,

생성된 상기 초기 비트열에 대해 일정 크기의 마스크를 적용하여 패리티 비트를 생성하되,

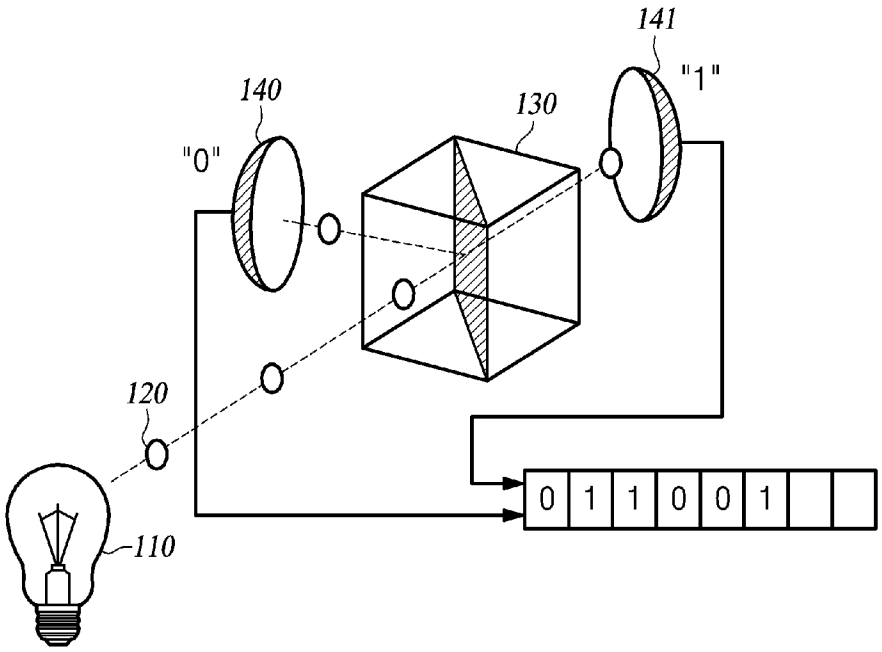
상기 마스크를 현재 패리티 비트를 생성한 위치로부터 적어도 1비트 이동하여 다음 패리티 비트를 생성하는 방식으로 연산함으로써 상기 난수를 생성하는 것을 특징으로 하는 광원 및

단일광자검출기를 이용한 난수 생성 방법.

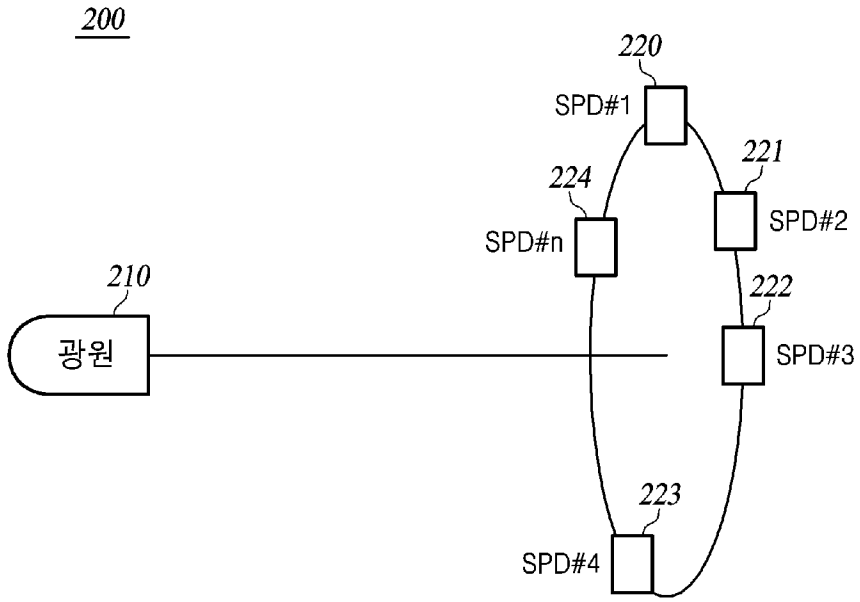
[청구항 20] 난수를 생성하는 장치에 있어서,
광원으로부터 출사된 광속으로부터 단일광자를 복수의 지점에서 검출하고, 상기 단일광자의 검출 여부를 0 또는 1의 디지털값으로 변환한 후 상기 디지털값에 수학적 연산을 취한 결과로써 난수를 생성하는 장치.

[청구항 21] 난수를 생성하는 방법에 있어서,
광원으로부터 출사된 광속으로부터 단일광자를 복수의 지점에서 검출하고, 상기 단일광자의 검출 여부를 0 또는 1의 디지털값으로 변환한 후 상기 디지털값에 수학적 연산을 취한 결과로써 난수를 생성하는 방법.

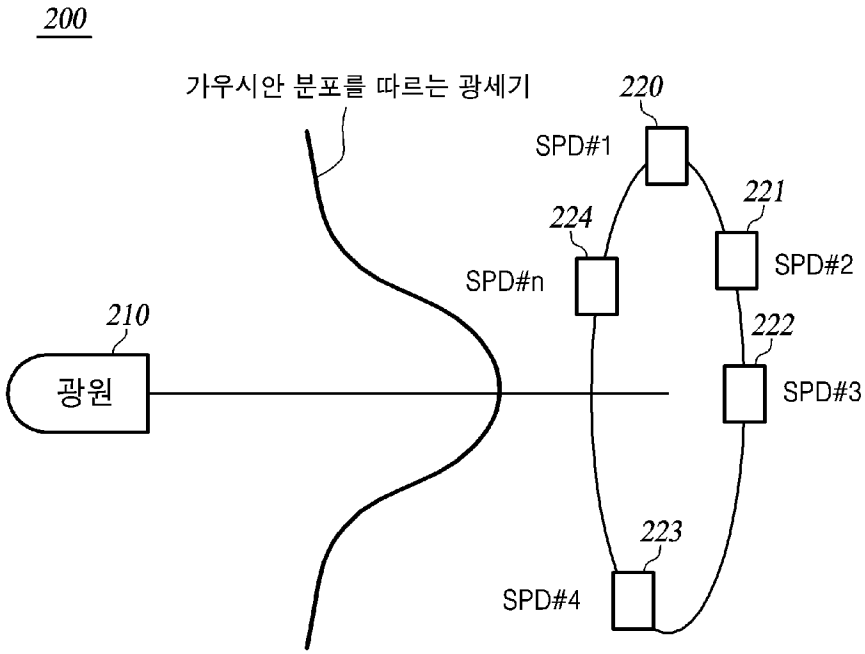
[Fig. 1]


141
"1"
140
130
"0"
120
0 1 1 0 0 1
110

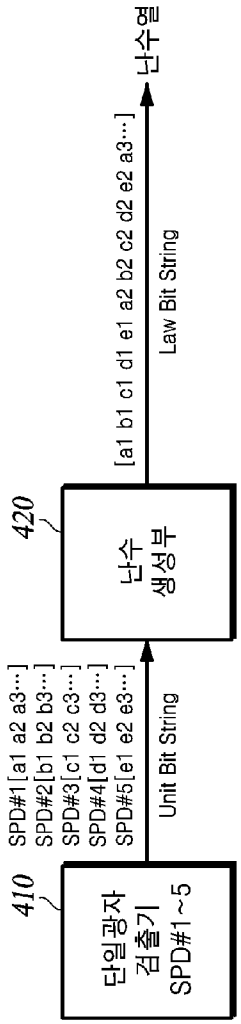
[Fig. 2]


200
220
SPD#1
221
224
SPD#2
SPD#n
210
222
광원
SPD#3
223
SPD#4

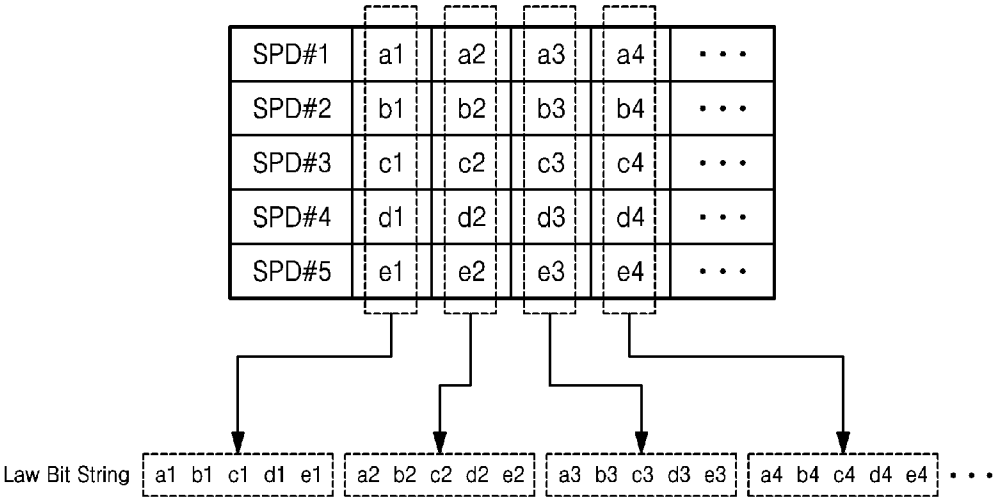
[Fig. 3]


200
가우시안 분포를 따르는 광세기
220
SPD#1
221
224
SPD#n
SPD#2
210
222
광원
SPD#3
223
SPD#4

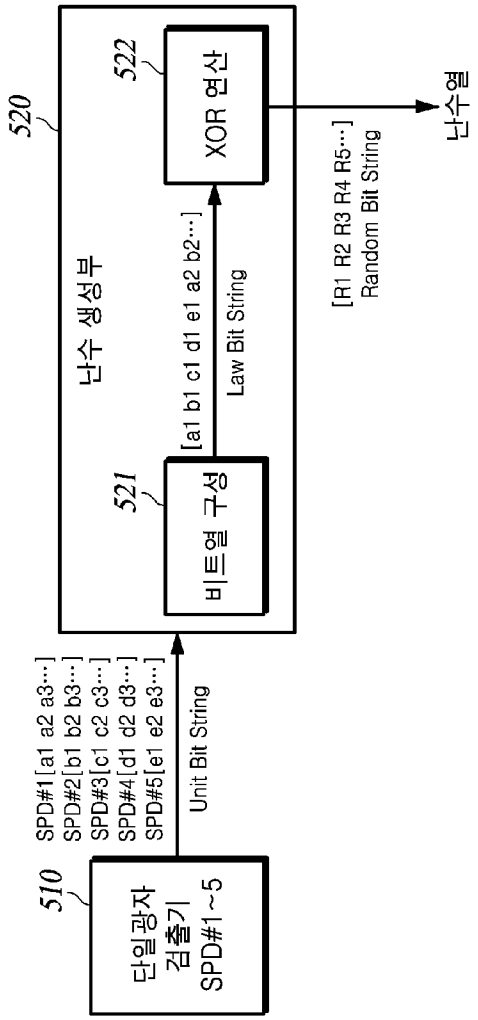
[Fig. 4a]


난수열
[a1 b1 c1 d1 e1 a2 b2 c2 d2 e2 a3…]
Law Bit String
420
난수 생성부
SPD#1[a1 a2 a3…]
SPD#2[b1 b2 b3…]
SPD#3[c1 c2 c3…]
SPD#4[d1 d2 d3…]
SPD#5[e1 e2 e3…]
Unit Bit String
410
단일광자 검출기 SPD#1~5

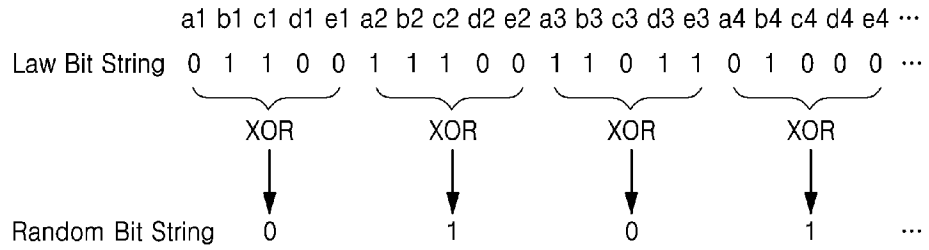
[Fig. 4b]


SPD#1 a1 a2 a3 a4 • • •
SPD#2 b1 b2 b3 b4 • • •
SPD#3 c1 c2 c3 c4 • • •
SPD#4 d1 d2 d3 d4 • • •
SPD#5 e1 e2 e3 e4 • • •
Law Bit String
a1 b1 c1 d1 e1
a2 b2 c2 d2 e2
a3 b3 c3 d3 e3
a4 b4 c4 d4 e4 • • •

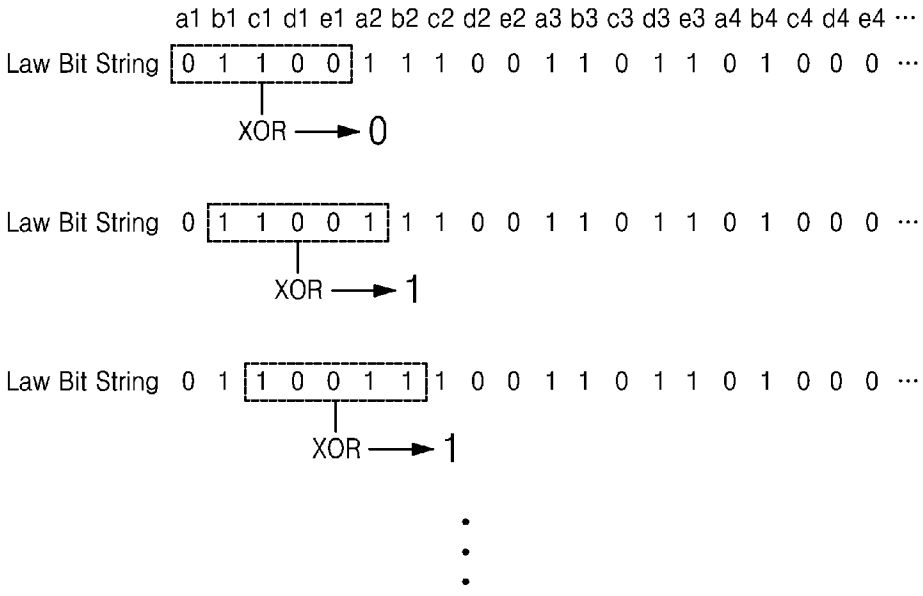
[Fig. 5a]


520
난수 생성부
522
XOR 연산
난수열
[R1 R2 R3 R4 R5…]
Random Bit String
[a1 b1 c1 d1 e1 a2 b2…]
Law Bit String
521
비트열 구성
SPD#1[a1 a2 a3…]
SPD#2[b1 b2 b3…]
SPD#3[c1 c2 c3…]
SPD#4[d1 d2 d3…]
SPD#5[e1 e2 e3…]
Unit Bit String
510
단일광자
검출기
SPD#1~5

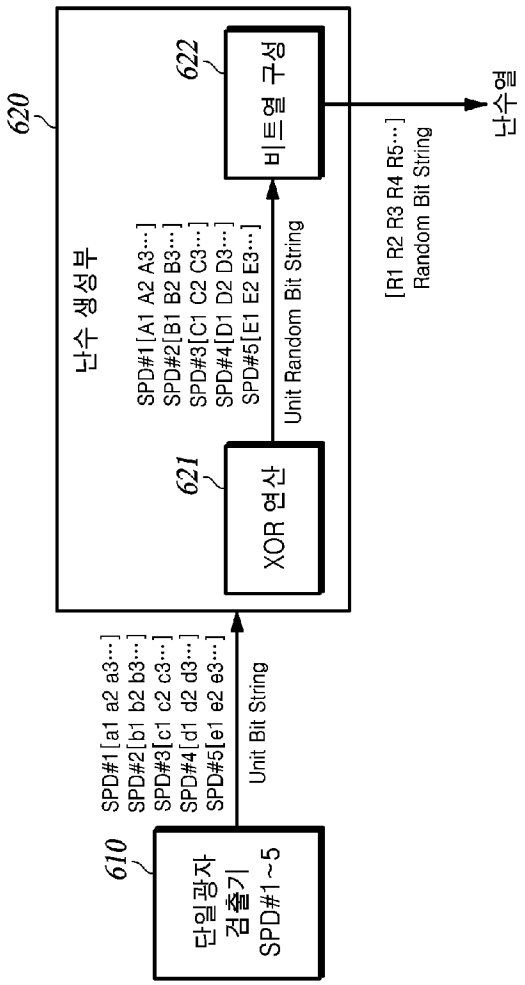
[Fig. 5b]


a1 b1 c1 d1 e1 a2 b2 c2 d2 e2 a3 b3 c3 d3 e3 a4 b4 c4 d4 e4 ···
Law Bit String 0 1 1 0 0 1 1 1 0 0 1 1 0 1 1 0 1 0 0 0 ···
XOR
XOR
XOR
XOR
Random Bit String 0 1 0 1 ···

[Fig. 5c]


a1 b1 c1 d1 e1 a2 b2 c2 d2 e2 a3 b3 c3 d3 e3 a4 b4 c4 d4 e4 ···
Law Bit String 0 1 1 0 0 1 1 1 0 0 1 1 0 1 1 0 1 0 0 0 ···
XOR → 0
Law Bit String 0 1 1 0 0 1 1 1 0 0 1 1 0 1 1 0 1 0 0 0 ···
XOR → 1
Law Bit String 0 1 1 0 0 1 1 1 0 0 1 1 0 1 1 0 1 0 0 0 ···
XOR → 1

[Fig. 6]


620
난수 생성부
610
단일광자 검출기 SPD#1~5
SPD#1[a1 a2 a3…]
SPD#2[b1 b2 b3…]
SPD#3[c1 c2 c3…]
SPD#4[d1 d2 d3…]
SPD#5[e1 e2 e3…]
Unit Bit String
621
XOR 연산
SPD#1[A1 A2 A3…]
SPD#2[B1 B2 B3…]
SPD#3[C1 C2 C3…]
SPD#4[D1 D2 D3…]
SPD#5[E1 E2 E3…]
Unit Random Bit String
622
비트열 구성
[R1 R2 R3 R4 R5…]
Random Bit String
난수열

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2013/007510

A. CLASSIFICATION OF SUBJECT MATTER

G06F 7/58(2006.01)i, G01J 1/02(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; H04K 1/00; G01R 15/22; H04L 9/12; H01S 3/00; H04B 10/04; G01J 1/02

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: generation of random number, light source, single photon detector, symmetrical distribution, radial shape separation, bit value, bit stream

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	US 2007-0127718 A1 (GREGOIRE, Ribordy et al.) 07 June 2007 See paragraphs [0029]-[0045]; claims 1 and 17; and figures 1-4.	1-3,6-8,13-16 ,20-21 4-5,9-12,17-19
A	US 2010-0217789 A1 (YOSHIAKI, Saitoh et al.) 26 August 2010 See paragraphs [0035] and [0039]-[0059]; and figures 1-2.	1-21
A	WO 2011-023501 A1 (UNIVERSITE LIBRE DE BRUXELLES) 03 March 2011 See page 8, lines 1-18; and figure 1.	1-21
A	JP 2007-129386 A (HITACHI LTD.) 24 May 2007 See paragraphs [0013]-[0016] and figure 1.	1-21
A	KR 10-1062790 B1 (HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P.) 07 September 2011 See paragraphs [0022]-[0032] and figure 1.	1-21

☐ 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
10 DECEMBER 2013 (10.12.2013)	**11 DECEMBER 2013 (11.12.2013)**
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.

Form PCT/ISA/210 (second sheet) (July 2009)

International application No.
PCT/KR2013/007510

Patent document cited in search report	Publication date	Patent family member	Publication date
US 2007-0127718 A1	07/06/2007	US 2005-0071400 A1	31/03/2005
		US 7447721 WD	04/11/2008
		US 7519641 B2	14/04/2009
US 2010-0217789 A1	26/08/2010	JP 4423431 B2	03/03/2010
		WO 2007-083417 A1	26/07/2007
WO 2011-023501 A1	03/03/2011	AU 2010-288722 A1	19/04/2012
		EP 2460069 A1	06/06/2012
		GB 0915000 D0	30/09/2009
		GB 0922156 D0	03/02/2010
		GB 2473078 A	02/03/2011
		JP 2013-503374 A	31/01/2013
		SG 178871 A1	27/04/2012
		US 2012-0221615 A1	30/08/2012
JP 2007-129386 A	24/05/2007	JP 4822811 B2	24/11/2011
		US 2008-0031637 A1	07/02/2008
		US 7738793 B2	15/06/2010
KR 10-1062790 B1	07/09/2011	CN 101473299 A	01/07/2009
		CN 101473299 B	03/08/2011
		CN 101479699 A	08/07/2009
		CN 101479699 B	17/11/2010
		CN 101529375 A	09/09/2009
		CN 101529375 B	11/07/2012
		EP 2013706 A2	14/01/2009
		EP 2013706 B1	06/07/2011
		EP 2013707 A2	14/01/2009
		EP 2013707 B1	06/07/2011
		EP 2013708 A2	14/01/2009
		EP 2013708 B1	16/10/2013
		JP 2009-534748 A	24/09/2009
		JP 2009-534750 A	24/09/2009
		JP 2010-501125 A	14/01/2010
		JP 4981126 B2	18/07/2012
		JP 5026508 B2	12/09/2012
		JP 5096457 B2	12/12/2012
		KR 10-0965970 B1	24/06/2010
		KR 10-0987885 B1	13/10/2010
		KR 10-2008-0111491 A	23/12/2008
		KR 10-2009-0012226 A	02/02/2009
		US 2007-0260658 A1	08/11/2007
		US 2008-0065710 A1	13/03/2008
		US 2008-0147759 A1	19/06/2008
		US 7844649 B2	30/11/2010
		US 7849121 B2	07/12/2010
		US 7849122 B2	07/12/2010
		WO 2007-124088 A2	01/11/2007

International application No.
PCT/KR2013/007510

Patent document cited in search report	Publication date	Patent family member	Publication date
		WO 2007-124088 A3	21/12/2007
		WO 2007-124089 A2	01/11/2007
		WO 2007-124089 A3	06/03/2008
		WO 2007-124121 A2	01/11/2007
		WO 2007-124121 A3	31/01/2008

국 제 조 사 보 고 서

국제출원번호
PCT/KR2013/007510

A. 발명이 속하는 기술분류(국제특허분류(IPC))

G06F 7/58(2006.01)i, G01J 1/02(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

G06F 7/58; H04K 1/00; G01R 15/22; H04L 9/12; H01S 3/00; H04B 10/04; G01J 1/02

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: 난수 생성, 광원, 단일광자검출기, 대칭분포, 방사상 이격, 비트값, 비트열

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
X A	US 2007-0127718 A1 (RIBORDY, GREGOIRE 외 1명) 2007.06.07 단락 [0029]-[0045]; 청구항 1과 17; 및 도면 1-4 참조.	1-3,6-8,13-16,20-21 4-5,9-12,17-19
A	US 2010-0217789 A1 (SAITOH, YOSHIAKI 외 1명) 2010.08.26 단락 [0035]과 [0039]-[0059]; 및 도면 1-2 참조.	1-21
A	WO 2011-023501 A1 (UNIVERSITE LIBRE DE BRUXELLES) 2011.03.03 페이지 8, 라인 1-18; 및 도면 1 참조.	1-21
A	JP 2007-129386 A (HITACHI LTD.) 2007.05.24 단락 [0013]-[0016] 및 도면 1 참조.	1-21
A	KR 10-1062790 B1 (휴렛-팩커드 디벨롭먼트 컴퍼니, 엘. 피.) 2011.09.07 단락 [0022]-[0032] 및 도면 1 참조.	1-21

☐ 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 12월 10일 (10.12.2013)	2013년 12월 11일 (11.12.2013)

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

심사관
노지명
전화번호 +82-42-481-8528

국제조사보고서
대응특허에 관한 정보

국제출원번호
PCT/KR2013/007510

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
US 2007-0127718 A1	2007/06/07	US 2005-0071400 A1	2005/03/31
		US 7447721 WD	2008/11/04
		US 7519641 B2	2009/04/14
US 2010-0217789 A1	2010/08/26	JP 4423431 B2	2010/03/03
		WO 2007-083417 A1	2007/07/26
WO 2011-023501 A1	2011/03/03	AU 2010-288722 A1	2012/04/19
		EP 2460069 A1	2012/06/06
		GB 0915000 D0	2009/09/30
		GB 0922156 D0	2010/02/03
		GB 2473078 A	2011/03/02
		JP 2013-503374 A	2013/01/31
		SG 178871 A1	2012/04/27
		US 2012-0221615 A1	2012/08/30
JP 2007-129386 A	2007/05/24	JP 4822811 B2	2011/11/24
		US 2008-0031637 A1	2008/02/07
		US 7738793 B2	2010/06/15
KR 10-1062790 B1	2011/09/07	CN 101473299 A	2009/07/01
		CN 101473299 B	2011/08/03
		CN 101479699 A	2009/07/08
		CN 101479699 B	2010/11/17
		CN 101529375 A	2009/09/09
		CN 101529375 B	2012/07/11
		EP 2013706 A2	2009/01/14
		EP 2013706 B1	2011/07/06
		EP 2013707 A2	2009/01/14
		EP 2013707 B1	2011/07/06
		EP 2013708 A2	2009/01/14
		EP 2013708 B1	2013/10/16
		JP 2009-534748 A	2009/09/24
		JP 2009-534750 A	2009/09/24
		JP 2010-501125 A	2010/01/14
		JP 4981126 B2	2012/07/18
		JP 5026508 B2	2012/09/12
		JP 5096457 B2	2012/12/12
		KR 10-0965970 B1	2010/06/24
		KR 10-0987885 B1	2010/10/13
		KR 10-2008-0111491 A	2008/12/23
		KR 10-2009-0012226 A	2009/02/02
		US 2007-0260658 A1	2007/11/08
		US 2008-0065710 A1	2008/03/13
		US 2008-0147759 A1	2008/06/19
		US 7844649 B2	2010/11/30
		US 7849121 B2	2010/12/07
		US 7849122 B2	2010/12/07
		WO 2007-124088 A2	2007/11/01

국제조사보고서
대응특허에 관한 정보

국제출원번호
PCT/KR2013/007510

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
		WO 2007-124088 A3	2007/12/21
		WO 2007-124089 A2	2007/11/01
		WO 2007-124089 A3	2008/03/06
		WO 2007-124121 A2	2007/11/01
		WO 2007-124121 A3	2008/01/31