(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2023-0021785
(43) 공개일자 2023년02월14일

(51) 국제특허분류(Int. Cl.)
G06F 7/58 (2006.01) *G01J 1/42* (2006.01)
H04L 9/08 (2006.01)
(52) CPC특허분류
G06F 7/58 (2018.05)
G01J 1/42 (2013.01)
(21) 출원번호 10-2021-0103556
(22) 출원일자 2021년08월06일
심사청구일자 2021년08월06일

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
허준
서울특별시 강남구 광평로10길 6, 206동 103호(일원동, 한솔마을아파트)
박주윤
서울특별시 성북구 보문로30나길 9, 102(동선동2가, 더스튜디오)
(74) 대리인
이대호, 박건홍

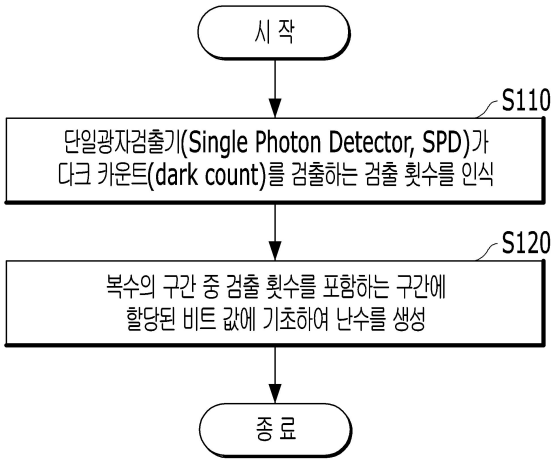
전체 청구항 수 : 총 14 항

(54) 발명의 명칭 **난수 생성 방법**

(57) 요 약

본 개시의 몇몇 실시예에 따른, 적어도 하나의 프로세서를 포함하는 컴퓨팅 장치에 의해 수행되는 난수 생성 방법이 개시된다. 상기 난수 생성 방법은 단일광자검출기(Single Photon Detector, SPD)가 다크 카운트(dark count)를 검출하는 검출 횟수를 인식하는 단계; 및 복수의 구간 중 상기 검출 횟수를 포함하는 구간에 할당된 비트 값에 기초하여 난수를 생성하는 단계를 포함할 수 있다.

대 표 도 - 도2



(52) CPC특허분류
H04L 9/0852 (2023.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711139206
과제번호	2021-0-01810-001
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	대학ICT연구센터육성지원사업
연구과제명	양자세계를 연결하는 초신뢰 양자인터넷 요소기술 개발
기 여 율	1/1
과제수행기관명	고려대학교산학협력단
연구기간	2021.07.01 ~ 2028.12.31

명 세 서

청구범위

청구항 1

적어도 하나의 프로세서를 포함하는 컴퓨팅 장치에 의해 수행되는 난수 생성 방법으로서,

단일광자검출기(Single Photon Detector, SPD)가 다크 카운트(dark count)를 검출하는 검출 횟수를 인식하는 단계; 및

복수의 구간 중 상기 검출 횟수를 포함하는 구간에 할당된 비트 값에 기초하여 난수를 생성하는 단계;

를 포함하는,

난수 생성 방법.

청구항 2

제 1 항에 있어서,

상기 복수의 구간은,

제 1 구간 및 제 2 구간을 포함하고,

상기 제 1 구간에 포함된 적어도 하나의 실수 값 각각 만큼 상기 다크 카운트가 검출될 확률의 총 합은,

상기 제 2 구간에 포함된 적어도 하나의 실수 값 각각 만큼 상기 다크 카운트가 검출될 확률의 총 합에 대응되는,

난수 생성 방법.

청구항 3

제 1 항에 있어서,

상기 단일광자검출기는,

기 설정된 시간 간격으로 트리거 신호가 인가된 경우, 상기 다크 카운트가 발생했는지 여부를 검출하는,

난수 생성 방법.

청구항 4

제 1 항에 있어서,

상기 복수의 구간 각각에 포함된 실수 값 각각 만큼 상기 다크 카운트가 검출될 확률 값은 정규 분포를 따르는,

난수 생성 방법.

청구항 5

제 1 항에 있어서,

상기 복수의 구간의 개수는,

사용자가 설정한 비트 크기에 기초하여 결정되는,

난수 생성 방법.

청구항 6

제 5 항에 있어서,

상기 비트 크기가 N인 경우, 상기 복수의 구간의 개수는 2^N개이고,

상기 N은 자연수인,

난수 생성 방법.

청구항 7

제 6 항에 있어서,

상기 복수의 구간 각각이 발생할 확률은,

$1/2^N$ 인,

난수 생성 방법.

청구항 8

다크 카운트(dark count)를 검출하는 단일광자검출기(Single Photon Detector, SPD); 및

프로세서;

를 포함하고,

상기 프로세서는,

단일광자검출기가 다크 카운트를 검출하는 검출 횟수를 인식하고,

복수의 구간 중 상기 검출 횟수를 포함하는 구간에 할당된 비트 값에 기초하여 난수를 생성하는,

난수 생성 장치.

청구항 9

제 8 항에 있어서,

상기 복수의 구간은,

제 1 구간 및 제 2 구간을 포함하고,

상기 제 1 구간에 포함된 적어도 하나의 실수 값 각각 만큼 상기 다크 카운트가 검출될 확률의 총 합은,

상기 제 2 구간에 포함된 적어도 하나의 실수 값 각각 만큼 상기 다크 카운트가 검출될 확률의 총 합에 대응되는,

난수 생성 장치.

청구항 10

제 8 항에 있어서,

상기 단일광자검출기는,

기 설정된 시간 간격으로 트리거 신호가 인가된 경우, 상기 다크 카운트가 발생했는지 여부를 검출하는,

난수 생성 장치.

청구항 11

제 8 항에 있어서,

상기 복수의 구간 각각에 포함된 실수 값 각각 만큼 상기 다크 카운트가 검출될 확률 값은 정규 분포를 따르는,

난수 생성 장치.

청구항 12

제 8 항에 있어서,

상기 복수의 구간의 개수는,

사용자가 설정한 비트 크기에 기초하여 결정되는,

난수 생성 장치.

청구항 13

제 12 항에 있어서,

상기 비트 크기가 N인 경우, 상기 복수의 구간의 개수는 2^N개이고,

상기 N은 자연수인,

난수 생성 장치.

청구항 14

제 13 항에 있어서,

상기 복수의 구간 각각이 발생할 확률은,

$1/2^N$ 인,

난수 생성 장치.

발명의 설명

기 술 분 야

[0001] 본 개시는 양자암호통신에 관한 것으로, 구체적으로 양자암호통신 구현에 불가피하게 발생하는 다크 카운트(dark count) 현상을 이용하여 난수를 생성하는 방법에 관한 것이다.

[0002] 본 연구는 과학기술정보통신부 및 정보통신기획평가원의 정보통신·방송 연구개발사업의 일환으로 수행하였다[2021-0-01810, 양자세계를 연결하는 초신뢰 양자인터넷 요소 기술 개발].

[0003] This work was supported by the ICT R&D program of MSIT/IITP[2021-0-01810, Development of elemental

technologies for Ultra-secure Quantum Internet].

배 경 기 술

[0004] 양자암호통신 구현에 사용하는 단일광자검출기(Single Photon Detector, SPD)는 제어신호에 의해서만 작동하는 Geiger mode 단일광자검출기와 제어신호 없이 항상 동작하고 있는 free running 단일광자검출기가 존재할 수 있다.

[0005] 양자암호통신에서 송신자와 수신자는 임의의 수열을 생성해야 할 필요가 있는데 이때 완전한 난수성을 보장하는 난수를 진난수라고 할 수 있으며, 진난수의 종류 중에 하나로 양자 난수가 존재할 수 있다. 여기서, 양자 난수는 사람이 아닌 순수 자연 현상의 물리계에서 추출하여 생성한 난수일 수 있다.

[0006] 한편, 단일광자검출기는 광자를 검출할 수 있는 광 검출기일 수 있다. 이러한 단일광자검출기의 성능을 방해하는 요소로서 다크 카운트(dark count) 현상이 존재할 수 있다. 여기서 다크 카운트란 실제로 단일광자검출기에 광신호가 전달되지 않을 때도 즉, 암전 상태에서 단일광자검출기를 동작시킨다 해도 생성되는 검출 신호일 수 있다. 이러한 다크 카운트에 의해 생성되는 검출 신호는 사용자에 의해 의도되지 않은 샷 노이즈(shot noise)에 의해 생성될 수 있다.

선행기술문헌

특허문헌

[0008] (특허문헌 0001) 대한민국 등록특허 10-1646506

발명의 내용

해결하려는 과제

[0009] 본 개시는 전술한 배경기술에 대응하여 안출된 것으로, 다크 카운트 현상을 이용하여 난수를 생성하는 방법을 제공하고자 한다.

[0010] 본 개시의 기술적 과제들은 이상에서 언급한 기술적 과제로 제한되지 않으며, 언급되지 않은 또 다른 기술적 과제들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0012] 전술한 바와 같은 과제를 해결하기 위한 본 개시의 일 실시예에 따라, 적어도 하나의 프로세서를 포함하는 컴퓨팅 장치에 의해 수행되는 난수 생성 방법이 개시된다. 상기 난수 생성 방법은 단일광자검출기(Single Photon Detector, SPD)가 다크 카운트(dark count)를 검출하는 검출 횟수를 인식하는 단계; 및 복수의 구간 중 상기 검출 횟수를 포함하는 구간에 할당된 비트 값에 기초하여 난수를 생성하는 단계; 를 포함할 수 있다.

[0013] 또한, 상기 복수의 구간은, 제 1 구간 및 제 2 구간을 포함하고, 상기 제 1 구간에 포함된 적어도 하나의 실수 값 각각 만큼 상기 다크 카운트가 검출될 확률의 총 합은, 상기 제 2 구간에 포함된 적어도 하나의 실수 값 각각 만큼 상기 다크 카운트가 검출될 확률의 총 합에 대응될 수 있다.

[0014] 또한, 상기 단일광자검출기는, 기 설정된 시간 간격으로 트리거 신호가 인가된 경우, 상기 다크 카운트가 발생했는지 여부를 검출할 수 있다.

[0015] 또한, 상기 복수의 구간 각각에 포함된 실수 값 각각 만큼 상기 다크 카운트가 검출될 확률 값은 정규 분포를 따를 수 있다.

[0016] 또한, 상기 복수의 구간의 개수는, 사용자가 설정한 비트 크기에 기초하여 결정될 수 있다.

[0017] 또한, 상기 비트 크기가 N인 경우, 상기 복수의 구간의 개수는 2^N개이고, 상기 N은 자연수일 수 있다.

[0018] 또한, 상기 복수의 구간 각각이 발생할 확률은, $^{1}/_{2^{N}}$ 일 수 있다.

[0019] 또한, 난수 생성 장치로서, 다크 카운트(dark count)를 검출하는 단일광자검출기(Single Photon Detector, SPD); 및 프로세서; 를 포함하고, 상기 프로세서는, 단일광자검출기가 다크 카운트를 검출하는 검출 횟수를 인식하고, 복수의 구간 중 상기 검출 횟수를 포함하는 구간에 할당된 비트 값에 기초하여 난수를 생성할 수 있다.

[0020] 또한, 상기 복수의 구간은, 제 1 구간 및 제 2 구간을 포함하고, 상기 제 1 구간에 포함된 적어도 하나의 실수 값 각각 만큼 상기 다크 카운트가 검출될 확률의 총 합은, 상기 제 2 구간에 포함된 적어도 하나의 실수 값 각각 만큼 상기 다크 카운트가 검출될 확률의 총 합에 대응될 수 있다.

[0021] 또한, 상기 단일광자검출기는, 기 설정된 시간 간격으로 트리거 신호가 인가된 경우, 상기 다크 카운트가 발생했는지 여부를 검출할 수 있다.

[0022] 또한, 상기 복수의 구간 각각에 포함된 실수 값 각각 만큼 상기 다크 카운트가 검출될 확률 값은 정규 분포를 따를 수 있다.

[0023] 또한, 상기 복수의 구간의 개수는, 사용자가 설정한 비트 크기에 기초하여 결정될 수 있다.

[0024] 또한, 상기 비트 크기가 N인 경우, 상기 복수의 구간의 개수는 2^{N}개이고, 상기 N은 자연수일 수 있다.

[0025] 또한, 상기 복수의 구간 각각이 발생할 확률은, $^{1}/_{2^{N}}$ 일 수 있다.

[0027] 본 개시에서 얻을 수 있는 기술적 해결 수단은 이상에서 언급한 해결 수단들로 제한되지 않으며, 언급하지 않은 또 다른 해결 수단들은 아래의 기재로부터 본 개시가 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

발명의 효과

[0029] 본 개시의 몇몇 실시예에 따르면, 별도의 장치나 비밀키를 소모하지 않고 양자 난수를 생성할 수 있는 방법을 제공할 수 있도록 한다.

[0030] 본 개시에서 얻을 수 있는 효과는 이상에서 언급한 효과로 제한되지 않으며, 언급하지 않은 또 다른 효과들은 아래의 기재로부터 본 개시가 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[0032] 다양한 양상들이 이제 도면들을 참조로 기재되며, 여기서 유사한 참조 번호들은 총괄적으로 유사한 구성요소들을 지칭하는데 이용된다. 이하의 실시예에서, 설명 목적을 위해, 다수의 특정 세부사항들이 하나 이상의 양상들의 총체적 이해를 제공하기 위해 제시된다. 그러나, 그러한 양상(들)이 이러한 특정 세부사항들 없이 실시될 수 있음은 명백할 것이다. 다른 예시들에서, 공지의 구조들 및 장치들이 하나 이상의 양상들의 기재를 용이하게 하기 위해 블록도 형태로 도시된다.

도 1은 본 개시의 몇몇 실시예에 따른 난수 생성 장치의 일례를 설명하기 위한 블록 구성도이다.

도 2는 본 개시의 몇몇 실시예에 따른 난수 생성 방법의 일례를 설명하기 위한 흐름도이다.

도 3은 본 개시의 몇몇 실시예에 따른 난수 생성 방법의 일례를 설명하기 위한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0033] 다양한 실시예들 및/또는 양상들이 이제 도면들을 참조하여 개시된다. 하기 설명에서는 설명을 목적으로, 하나 이상의 양상들의 전반적 이해를 돕기 위해 다수의 구체적인 세부사항들이 개시된다. 그러나, 이러한 양상(들)은 이러한 구체적인 세부사항들 없이도 실행될 수 있다는 점 또한 본 개시의 기술 분야에서 통상의 지식을 가진 자

에게 감지될 수 있을 것이다. 이후의 기재 및 첨부된 도면들은 하나 이상의 양상들의 특정한 예시적인 양상들을 상세하게 기술한다. 하지만, 이러한 양상들은 예시적인 것이고 다양한 양상들의 원리들에서의 다양한 방법들 중 일부가 이용될 수 있으며, 기술되는 설명들은 그러한 양상들 및 그들의 균등물들을 모두 포함하고자 하는 의도이다. 구체적으로, 본 명세서에서 사용되는 "실시예", "예", "양상", "예시" 등은 기술되는 임의의 양상 또는 설계가 다른 양상 또는 설계들보다 양호하다거나, 이점이 있는 것으로 해석되지 않을 수도 있다.

[0034] 이하, 도면 부호에 관계없이 동일하거나 유사한 구성 요소는 동일한 참조 번호를 부여하고 이에 대한 중복되는 설명은 생략한다. 또한, 본 명세서에 개시된 실시예를 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 본 명세서에 개시된 실시예의 요지를 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다. 또한, 첨부된 도면은 본 명세서에 개시된 실시예를 쉽게 이해할 수 있도록 하기 위한 것일 뿐, 첨부된 도면에 의해 본 명세서에 개시된 기술적 사상이 제한되지 않는다.

[0035] 비록 제 1, 제 2 등이 다양한 소자나 구성요소들을 서술하기 위해서 사용되나, 이들 소자나 구성요소들은 이들 용어에 의해 제한되지 않음은 물론이다. 이들 용어들은 단지 하나의 소자나 구성요소를 다른 소자나 구성요소와 구별하기 위하여 사용하는 것이다. 따라서, 이하에서 언급되는 제 1 소자나 구성요소는 본 발명의 기술적 사상 내에서 제 2 소자나 구성요소 일 수도 있음은 물론이다.

[0036] 다른 정의가 없다면, 본 명세서에서 사용되는 모든 용어(기술 및 과학적 용어를 포함)는 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에게 공통적으로 이해될 수 있는 의미로 사용될 수 있을 것이다. 또 일반적으로 사용되는 사전에 정의되어 있는 용어들은 명백하게 특별히 정의되어 있지 않는 한 이상적으로 또는 과도하게 해석되지 않는다.

[0037] 더불어, 용어 "또는"은 배타적 "또는"이 아니라 내포적 "또는"을 의미하는 것으로 의도된다. 즉, 달리 특정되지 않거나 문맥상 명확하지 않은 경우에, "X는 A 또는 B를 이용한다"는 자연적인 내포적 치환 중 하나를 의미하는 것으로 의도된다. 즉, X가 A를 이용하거나; X가 B를 이용하거나; 또는 X가 A 및 B 모두를 이용하는 경우, "X는 A 또는 B를 이용한다"가 이들 경우들 어느 것으로도 적용될 수 있다. 또한, 본 명세서에 사용된 "및/또는"이라는 용어는 열거된 관련 아이템들 중 하나 이상의 아이템의 가능한 모든 조합을 지칭하고 포함하는 것으로 이해되어야 한다.

[0038] 또한, "포함한다" 및/또는 "포함하는"이라는 용어는, 해당 특징 및/또는 구성요소가 존재함을 의미하지만, 하나 이상의 다른 특징, 구성요소 및/또는 이들의 그룹의 존재 또는 추가를 배제하지 않는 것으로 이해되어야 한다. 또한, 달리 특정되지 않거나 단수 형태를 지시하는 것으로 문맥상 명확하지 않은 경우에, 본 명세서와 청구범위에서 단수는 일반적으로 "하나 또는 그 이상"을 의미하는 것으로 해석되어야 한다.

[0039] 더불어, 본 명세서에서 사용되는 용어 "정보" 및 "데이터"는 종종 서로 상호교환 가능하도록 사용될 수 있다.

[0040] 어떤 구성 요소가 다른 구성 요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성 요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성 요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성 요소가 다른 구성 요소에 "직접 연결되어" 있다거나 "직접 접속되어"있다고 언급된 때에는, 중간에 다른 구성 요소가 존재하지 않는 것으로 이해되어야 할 것이다.

[0041] 이하의 설명에서 사용되는 구성 요소에 대한 접미사 "모듈" 및 "부"는 명세서 작성의 용이함만이 고려되어 부여되거나 혼용되는 것으로서 그 자체로 서로 구별되는 의미 또는 역할을 갖는 것은 아니다.

[0042] 본 개시의 목적 및 효과, 그리고 그것들을 달성하기 위한 기술적 구성들은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 본 개시를 설명하는데 있어서 공지 기능 또는 구성에 대한 구체적인 설명이 본 개시의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다. 그리고 후술되는 용어들은 본 개시에서의 기능을 고려하여 정의된 용어들로써 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다.

[0043] 그러나 본 개시는 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있다. 단지 본 실시예들은 본 개시가 완전하도록 하고, 본 개시가 속하는 기술분야에서 통상의 지식을 가진 자에게 개시의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 개시는 청구항의 범주에 의해 정의될 뿐이다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

[0045] 본 개시에서, 난수 생성 장치는 단일광자검출기(Single Photon Detector, SPD)를 포함할 수 있다. 애벌런치 포

토다이오드(Avalanche photodiode)를 사용하는 단일광자검출기를 이용하여 빛을 검출하는 경우, 실제로 빛이 들어오지 않아도 검출 신호를 출력하는 다크 카운트(dark count) 현상이 발생할 수 있다. 여기서, 애벌런치 포토 다이오드는 내부에 광 전류의 증폭 기구를 가진 포토 다이오드로서, 일반적으로 광검출기로 많이 사용되는 포토 다이오드일 수 있다. 한편, 상기한 바와 같이 다크 카운트 현상은 실제로 단일광자검출기에 광신호가 전달되지 않을 때도 즉, 암전상태에서 단일광자검출기를 동작시킨다 해도 발생할 수 있다. 그리고, 이러한 다크 카운트 현상은 일종의 노이즈에 의해 발생되는 현상으로서, 사용자에 의해 의도되지 않은 현상일 수 있다. 따라서, 다크 카운트 현상의 발생 횟수를 이용하여 난수를 생성하는 경우, 생성되는 난수는 진난수 일 수 있다. 이하, 본 개시에 따른 난수 생성 방법에 대해 도 1 내지 도 3을 통해 설명한다.

[0047] 도 1은 본 개시의 몇몇 실시예에 따른 난수 생성 장치의 일례를 설명하기 위한 블록 구성도이다.

[0048] 도 1을 참조하면, 난수 생성 장치(100)는 단일광자검출기(110) 및 프로세서(120)를 포함할 수 있다. 다만, 상술한 구성 요소들은 난수 생성 장치(100)를 구현하는데 있어서 필수적인 것은 아니어서, 난수 생성 장치(100)는 위에서 열거된 구성요소들 보다 많거나, 또는 적은 구성요소들을 가질 수 있다.

[0049] 난수 생성 장치(100)는 양자 암호 통신을 구현하는 컴퓨팅 장치일 수 있다. 다만, 이에 한정되는 것은 아니다.

[0050] 단일광자검출기(110)는 광자를 검출할 수 있는 장치로서, 본 개시에서의 단일광자검출기(110)는 다크 카운트 현상(이하, 다크 카운트)을 검출할 수 있다. 실시예에 따라, 단일광자검출기(110)는 기 설정된 시간 간격으로 트리거(trigger) 신호가 인가된 경우, 다크 카운트가 발생했는지 여부를 검출할 수 있다. 일례로, 단일광자검출기(110)는 암전 상태에서 기 설정된 시간 간격으로 트리거 신호가 인가될 수 있다. 그리고, 암전 상태에서 트리거 신호가 인가되었음에도 불구하고 검출 신호가 생성된 경우, 단일광자검출기(110)는 다크 카운트가 발생했다고 인식할 수 있다. 다만, 이에 한정되는 것은 아니다.

[0051] 한편, 프로세서(120)는 통상적으로 난수 생성 장치(100)의 전반적인 동작을 제어할 수 있다. 프로세서(120)는 위에서 살펴본 구성요소들을 통해 입력 또는 출력되는 신호, 데이터, 정보 등을 처리하거나 데이터베이스(미도시)에 저장된 응용 프로그램을 구동함으로써, 사용자에게 적절한 정보 또는 기능을 제공 또는 처리할 수 있다.

[0052] 본 개시에서, 프로세서(120)는 단일광자검출기(110)를 통해 다크 카운트가 검출된 검출 횟수를 인식한 경우, 복수의 구간 중 검출 횟수를 포함하는 구간에 할당된 비트 값에 기초하여 난수를 생성할 수 있다.

[0053] 구체적으로, 다크 카운트가 발생하는 확률을 p(p는 소수(decimal) 또는 자연수)라고 정의하고, 기 설정된 시간 간격으로 m(m은 자연수)개의 트리거(trigger) 신호가 단일광자검출기(110)에 인가되는 경우, 해당 시간에 다크 카운트가 검출되는 확률 변수(random variable)는 이항분포 $x_i \sim B(m,p)$를 따를 수 있다. 여기서, 트리거 신호는 광자의 검출을 위하여 또는 다크 카운트의 검출을 위하여 단일광자검출기(110)에 인가되는 신호일 수 있다. 또한, 해당 시간은 m개의 트리거 신호가 모두 인가된 시간일 수 있다.

[0054] 한편, m이 충분히 큰 수 인 경우, 즉 트리거 신호의 개수가 충분히 많은 개수인 경우, 확률변수 x_i의 합인 X는 정규분포 $X \sim M(mp, mp(1-p))$를 따를 수 있다. 여기서, 확률변수 x_i의 합인 X는 $X = \sum_{i=1}^{m} x_i$와 같이 도출될 수 있다. 즉, 충분한 시간만큼 다크 카운트가 발생했는지 여부를 검출하는 경우, 다크 카운트가 각각의 횟수만큼 검출될 확률 값은 정규 분포를 따를 수 있다.

[0055] 한편, 본 개시에서는, 프로세서(120)는 다크 카운트가 검출된 횟수를 이용하여 복수의 구간을 생성할 수 있다. 여기서, 충분한 시간만큼 다크 카운트가 발생했는지 여부를 검출하는 경우, 다크 카운트가 각각의 횟수만큼 검출될 확률 값이 정규 분포를 따르기 때문에, 복수의 구간 각각에 포함된 실수 값 각각 만큼 다크 카운트가 검출될 확률 값도 정규 분포를 따를 수 있다.

[0056] 예를 들어, 프로세서(120)는 1 내지 7의 실수 값을 제 1 구간으로 나누고, 8 내지 9의 실수 값을 제 2 구간으로 나누며, 10 내지 11의 실수 값을 제 3 구간으로 나누고, 나머지 실수 값(12 내지 100)을 제 4 구간으로 나눌 수 있다. 그리고, 각각의 구간에 포함된 실수 값은 충분한 시간 동안 다크 카운트가 발생되는 횟수를 의미할 수 있다. 따라서, 복수의 구간 각각에 포함된 실수 값 각각 만큼 다크 카운트가 검출될 확률 값은 정규 분포를 따를 수 있다. 그리고, 프로세서(120)는 복수의 구간이 나누어진 경우, 복수의 구간 각각에 비트 값을 할당할 수 있다. 이 경우, 프로세서(120)는 복수의 구간 중 단일광자검출기(110)가 다크 카운트를 검출한 검출 횟수를 포함

하는 구간에 할당된 비트 값에 기초하여 난수를 생성할 수 있다. 즉, 프로세서(120)는 의도치 않게 단일광자검출기(110)에서 검출되는 다크 카운트를 이용하여 난수를 생성할 수 있다. 따라서, 생성되는 난수는 진난수일 수 있다. 이하, 도 2 내지 도 3을 통해 프로세서(120)가 난수를 생성하는 방법에 대해 좀 더 설명한다.

[0058] 도 2는 본 개시의 몇몇 실시예에 따른 난수 생성 장치가 난수를 생성하는 방법의 일례를 설명하기 위한 흐름도이다. 도 3은 본 개시의 몇몇 실시예에 따른 난수 생성 방법의 일례를 설명하기 위한 도면이다.

[0059] 도 2를 참조하면, 난수 생성 장치(100)의 프로세서(120)는 단일광자검출기(110)가 다크 카운트를 검출하는 검출 횟수를 인식할 수 있다(S110).

[0060] 일례로, 프로세서(120)는 암전 상태에서의 단일광자검출기(110)에 기 설정된 시간 간격으로 트리거 신호를 인가할 수 있다. 그리고, 암전 상태에서 트리거 신호가 인가되었음에도 불구하고 단일광자검출기(110)에 의해 검출 신호가 생성된 경우, 프로세서(120)는 다크 카운트가 발생했다고 인식할 수 있다. 이 경우, 프로세서(120)는 검출 신호가 생성된 횟수를 다크 카운트가 검출된 검출 횟수라고 인식할 수 있다. 다만, 이에 한정되는 것은 아니다.

[0061] 한편, 난수 생성 장치(100)의 프로세서(120)는 복수의 구간 중 검출 횟수를 포함하는 구간에 할당된 비트 값에 기초하여 난수를 생성할 수 있다(S120).

[0062] 일례로, 도 3을 참조하면, m은 100이고, p는 0.1인 경우, X는 정규분포 $N(10,9)$를 따를 수 있다. 이 경우, 프로세서(120)는 제 1 구간(210) 내지 제 4 구간(240)을 포함하는 복수의 구간을 생성할 수 있다. 예를 들어, 프로세서(120)는 1 내지 7의 실수 값을 제 1 구간(210)으로 나누고, 8 내지 9의 실수 값을 제 2 구간(220)으로 나누며, 10 내지 11의 실수 값을 제 3 구간(230)으로 나누고, 12 내지 100의 실수 값을 제 4 구간(240)으로 나눌 수 있다. 그리고, 복수의 구간이 생성된 경우, 프로세서(120)는 복수의 구간 각각에 비트 값을 할당할 수 있다. 실시예에 따라, 프로세서(120)는 제 1 구간(210)에는 제 1 비트 값(310)을 할당하고, 제 2 구간(220)에는 제 2 비트 값(320)을 할당할 수 있다. 또한, 프로세서(120)는 제 3 구간(230)에는 제 3 비트 값(330)을 할당하고, 제 4 구간(240)에는 제 4 비트 값(340)을 할당할 수 있다. 이에 따라, 프로세서(120)는 검출 횟수가 인식된 경우, 제 1 구간(210) 내지 제 4 구간(240) 중 검출 횟수를 포함하는 구간에 할당된 비트 값을 결정할 수 있다.

[0063] 예를 들어, 프로세서(120)는 m회의 시행 횟수를 통해 단일광자검출기(110)가 다크 카운트를 검출한 검출 횟수는 6회라고 인식할 수 있다. 이 경우, 프로세서(120)는 복수의 구간 중 6회의 검출 횟수를 포함하는 구간이 제 1 구간(210)이라고 결정할 수 있다. 이에 따라, 프로세서(120)는 제 1 구간(210)에 할당된 제 1 비트 값(310)을 인식하고, 제 1 비트 값(310)에 기초하여 난수를 생성할 수 있다. 다만, 이에 한정되는 것은 아니다.

[0064] 본 개시의 몇몇 실시예에 따르면, 프로세서(120)는 m회의 시행 횟수를 통해 다크 카운트를 검출하는 동작을 k(k는 자연수)회 수행할 수 있다. 이 경우, 프로세서 k회의 동작을 수행하는 동안 결정된 비트 값에 기초하여 난수를 생성할 수 있다. 일례로, k가 3인 경우, 프로세서(120)는 첫번째 m회의 시행 횟수를 통해 단일광자검출기(110)가 다크 카운트를 검출한 검출 횟수에 기초하여, 제 1 비트 값(310)을 결정할 수 있다. 그리고, 프로세서(120)는 두번째 m회의 시행 횟수를 통해 단일광자검출기(110)가 다크 카운트를 검출한 검출 횟수에 기초하여, 제 2 비트 값(320)을 결정할 수 있다. 또한, 프로세서(120)는 세번째 m회의 시행 횟수를 통해 단일광자검출기(110)가 다크 카운트를 검출한 검출 횟수에 기초하여, 제 1 비트 값(310)을 결정할 수 있다. 이 경우, 프로세서(120)는 "000100"과 같은 난수를 생성할 수 있다. 다만, 이에 한정되는 것은 아니다.

[0065] 한편, 본 개시의 몇몇 실시예에 따르면, 복수의 구간은 제 1 구간(210) 및 제 2 구간(220)을 포함할 수 있다. 이 경우, 제 1 구간(210)에 포함된 적어도 하나의 실수 값 각각 만큼 다크 카운트가 검출될 확률의 총 합은 제 2 구간(220)에 포함된 적어도 하나의 실수 값 각각 만큼 다크 카운트가 검출될 확률의 총 합에 대응될 수 있다. 실시예에 따라, 복수의 구간은 제 1 구간(210) 내지 제 4 구간(240)을 포함할 수 있다. 이 경우, 각각의 구간에 포함된 적어도 하나의 실수 값 각각 만큼 다크 카운트가 검출될 확률의 총 합은 서로 대응될 수 있다.

[0066] 구체적으로, X의 확률 분포인 $p(X)$(400)를 참조하면, 제 1 구간(210)에 포함된 적어도 하나의 실수 값 각각 만큼 다크 카운트가 검출될 확률의 총 합은 0.2525일 수 있다. 그리고, 제 2 구간(220)에 포함된 적어도 하나의 실수 값 각각 만큼 다크 카운트가 검출될 확률의 총 합은 0.2475일 수 있다. 또한, 제 3 구간(230)에 포함된 적

어도 하나의 실수 값 각각 만큼 다크 카운트가 검출될 확률의 총 합은 0.2475일 수 있다. 그리고, 제 4 구간(240)에 포함된 적어도 하나의 실수 값 각각 만큼 다크 카운트가 검출될 확률의 총 합은 0.2525일 수 있다. 즉, 각각의 구간에 포함된 적어도 하나의 실수 값 각각 만큼 다크 카운트가 검출될 확률의 총 합은 서로 대응될 수 있다. 여기서, 다크 카운트가 검출될 확률의 총 합은 서로 대응될 수 있다는 것은 서로 유사(총 합의 차이가 0.01 이하)하거나 또는 동일할 수 있다는 의미일 수 있다. 상술한 예시에서는 이해를 돕기 위하여 m이 100인 경우를 예를 들어 설명함에 따라 각 구간의 다크 카운트가 검출될 확률의 총 합이 서로 유사하게 결정될 수 있었다. 그러나, m이 충분히 큰 수인 경우, 다크 카운트가 검출될 확률의 총 합은 서로 동일하게 결정될 수도 있다. 다만, 이에 한정되는 것은 아니다.

[0067] 한편, 본 개시의 몇몇 실시예에 따르면, 복수의 구간의 개수는 사용자가 설정한 비트 크기에 기초하여 결정될 수 있다.

[0068] 구체적으로, 프로세서(120)는 사용자 입력부 등을 통해 사용자로부터 비트 크기를 입력 받을 수 있다. 이 경우, 프로세서(120)는 사용자에 의해 설정된 비트 크기에 기초하여 복수의 구간의 개수를 결정할 수 있다. 일례로, 비트 크기가 N(N은 자연수)인 경우, 복수의 구간의 개수는 2^N개일 수 있다.

[0069] 예를 들어, 제 1 비트 값(310)을 참조하면, 제 1 비트 값(310)은 "00"일 수 있다. 따라서, 제 1 비트 값의 크기는 2일 수 있다. 즉, 프로세서(120)는 사용자로부터 2개 또는 2의 크기를 갖는 비트를 생성한다고 입력 받았을 수 있다. 이 경우, 프로세서(120)는 사용자로부터 입력 받은 비트 크기에 기초하여, 복수의 구간을 2^2개인 4개로 나눌 수 있다. 다만, 이에 한정되는 것은 아니다.

[0070] 한편, 본 개시의 몇몇 실시예에 따르면, 복수의 구간 각각이 발생할 확률은 $1/2^N$ 일 수 있다. 일례로, 난수 생성 장치(100)의 프로세서(120)는 사용자로부터 2개의 비트를 생성한다고 입력 받은 경우, 복수의 구간 각각이 발생할 확률이 $1/2^2$이 될 수 있도록 복수의 구간을 나눌 수 있다. 이 경우, 다크 카운트가 검출될 확률의 총 합은 서로 동일할 수 있다. 다만, 이에 한정되는 것은 아니다.

[0071] 한편, 본 개시의 몇몇 실시예에 따르면, 난수 생성 장치(100)의 프로세서(120)는 난수의 생성속도를 구할 수도 있다. 이 경우, 사용자는 난수가 생성되는 속도를 고려하여, 본 개시에 따른 난수를 생성하는 작업을 수행할지 여부를 결정할 수도 있다.

[0072] 구체적으로, 실시예에 따라 m은 100이고, p는 0.1인 경우, X의 확률 분포인 $p(X)$(400)는 도 3에 도시된 바와 같이 결정될 수 있다. 이 경우, 프로세서(120)가 X의 값에 해당하는 구역에 비트를 할당한다면 정해진 횟수인 100회 동안 2개의 임의의 비트를 얻을 수 있다. 프로세서(120)가 100㎒로 트리거 신호를 단일광자검출기(110)에 입력한다고 가정하면, 시행 횟수는 1초를 기준으로 10^8번일 수 있다. 그리고, 정해진 횟수(또는 간격)인 100회 단위로 각 구간을 보면, 10^6개의 구간이 생성될 수 있다. 이 경우, 한 구간에 2개의 비트가 생성되므로, 프로세서(120)가 생성하는 난수의 생성속도는 2㎒가 될 수 있다.

[0073] 실시예에 따라, 현실적인 단일광자검출기(110)의 성능에 기초하여, $p = 1.7 \times 10^{-6}$이라고 가정하고, $n = 5 \times 10^{-6}$이라고 가정하고, 단일광자검출기(110)의 동작속도는 100㎒라고 가정할 수 있다. 이 경우, 프로세서(120)가 생성하는 난수의 생성속도는 40b/s로 계산될 수 있다. 다만, 이는 실시예일 뿐, 프로세서(120)가 생성하는 난수의 생성속도는 단일광자검출기(110)의 성능에 따라 결정될 수 있다.

[0074] 한편, 본 개시의 몇몇 실시예에 따르면, 난수 생성 장치(100)의 프로세서(120)가 난수를 생성하는 속도는 비트를 할당하는 구간에 기초하여 결정될 수도 있다.

[0075] 구체적으로, 프로세서(120)는 사용자로부터의 입력에 기초하여, 복수의 구간 각각이 발생할 확률이 $1/8$이 되도록 결정할 수 있다. 즉, 프로세서(120)는 사용자로부터 매 구간 마다 3개의 비트를 생성하도록 비트 크기를 입력 받았을 수 있다. 이에 따라, 프로세서(120)는 비트 크기에 기초하여, 복수의 구간 각각이 발생할 확률이 $1/2^3$개가 되도록 결정할 수 있다. 그리고, $p = 1.7 \times 10^{-6}$이라고 가정하고, $n = 5 \times 10^{-6}$이라고 가정하고, 단일광자검출기(110)의 동작속도는 100㎒라고 가정하는 경우, 프로세서(120)가 생성하는 난수생성 속도는 60b/s일

수 있다. 다만, 이에 한정되는 것은 아니다.

[0076] 상술한 내용에 따르면, 난수 생성 장치(100)는 복수의 구간 중 단일광자검출기(110)가 다크 카운트를 검출한 검출 횟수를 포함하는 구간에 할당된 비트 값에 기초하여 난수를 생성할 수 있다. 즉, 난수 생성 장치(100)는 의도치 않게 단일광자검출기(110)에서 검출되는 다크 카운트를 이용하여 난수를 생성할 수 있다. 따라서, 생성되는 난수는 진난수일 수 있으며, 이를 활용하여 양자암호통신을 수행하는 경우, 안전한 통신이 가능할 수 있다.

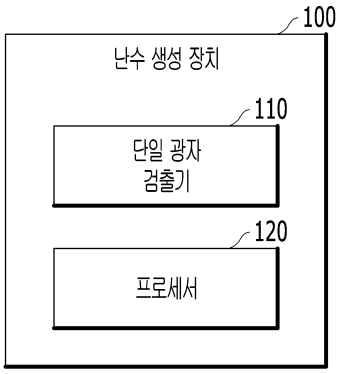
[0077] 또한, 기존의 양자암호통신에서 사용되는 난수는 따로 준비된 양자난수생성기 혹은 양자통신에 의하여 생성된 임의의 비밀키 일부를 사용하는 방법을 통해 만들어질 수 있었다. 이 경우 별도의 양자난수생성기가 필요하거나 비밀키 일부를 소모해야 해서 키 생성률이 줄어들 수 있다는 문제점이 존재할 수 있었다.

[0078] 반면, 상술한 내용에 따르면 별도의 장치가 필요하지 않기 때문에 비용을 절감할 수 있고, 비밀키의 일부를 사용하지 않음에 따라 키 생성률이 높아지기 때문에 더 안전한 통신을 가능하게 할 수 있다. 구체적으로, 키 생성률이 높아지면 더 안전한 통신을 할 수 있는 이유는 키 생성률은 암호통신 거리가 증가할수록 줄어들게 되는데 키 생성률이 높아진다면 더 멀리 암호키를 주고받을 수 있기 때문일 수 있다. 따라서, 본 개시에 따른 난수 생성 장치(100)를 활용하는 경우, 더욱 더 안전한 통신이 가능할 수 있다.

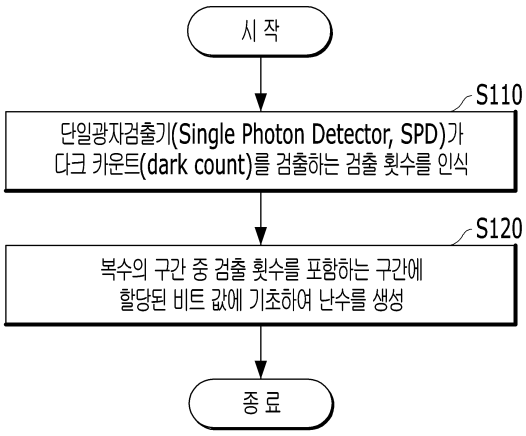
[0080] 제시된 실시예들에 대한 설명은 임의의 본 개시의 기술 분야에서 통상의 지식을 가진 자가 본 개시를 이용하거나 또는 실시할 수 있도록 제공된다. 이러한 실시예들에 대한 다양한 변형들은 본 개시의 기술 분야에서 통상의 지식을 가진 자에게 명백할 것이며, 여기에 정의된 일반적인 원리들은 본 개시의 범위를 벗어남이 없이 다른 실시예들에 적용될 수 있다. 그리하여, 본 개시는 여기에 제시된 실시예들로 한정되는 것이 아니라, 여기에 제시된 원리들 및 신규한 특징들과 일관되는 최광의의 범위에서 해석되어야 할 것이다.

도면

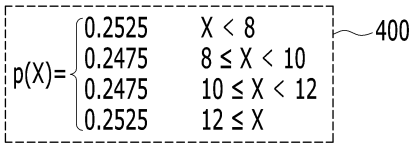
도면1

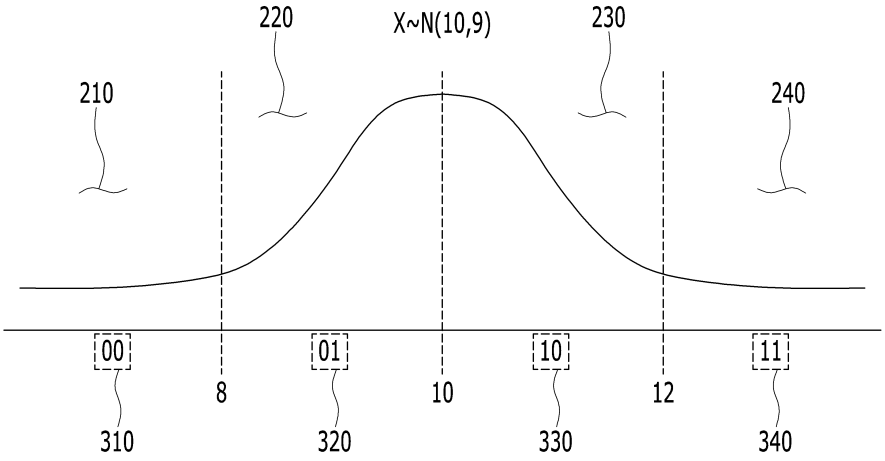


도면2


시 작
S110
단일광자검출기(Single Photon Detector, SPD)가
다크 카운트(dark count)를 검출하는 검출 횟수를 인식
S120
복수의 구간 중 검출 횟수를 포함하는 구간에
할당된 비트 값에 기초하여 난수를 생성
종 료

도면3


p(X)=
0.2525 X < 8
0.2475 8 ≤ X < 10
0.2475 10 ≤ X < 12
0.2525 12 ≤ X
400


220
X~N(10,9)
230
210
240
00
01
10
11
8
10
12
310
320
330
340