(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2024년01월18일
(11) 등록번호 10-2626031
(24) 등록일자 2024년01월12일

(51) 국제특허분류(Int. Cl.)
G06F 7/58 (2006.01) *G06N 99/00* (2019.01)
H01S 3/11 (2023.01) *H01S 5/062* (2006.01)
H01S 5/065 (2006.01) *H01S 5/30* (2006.01)
(52) CPC특허분류
G06F 7/588 (2013.01)
G06N 10/00 (2022.01)
(21) 출원번호 10-2018-7014879
(22) 출원일자(국제) 2016년09월28일
심사청구일자 2021년09월16일
(85) 번역문제출일자 2018년05월25일
(65) 공개번호 10-2018-0073663
(43) 공개일자 2018년07월02일
(86) 국제출원번호 PCT/EP2016/073099
(87) 국제공개번호 WO 2017/071901
국제공개일자 2017년05월04일
(30) 우선권주장
14/923,495 2015년10월27일 미국(US)
(56) 선행기술조사문헌
JP2013503374 A
WO2007083417 A1
JP2009230200 A
US20130036145 A1

(73) 특허권자
푼다시오 인스티튜트 드 시엔시스 포토닉스
스페인, (바르셀로나) 카스텔데펠스 08860, 넘 3, 에이브이. 칼 프리드리히 가우스
인스티튜시오 카탈라나 드 르세르카 아이 에스투디스 아반카츠
스페인 이-08010 바르셀로나 23 패세익 루이스 컴파니스
(72) 발명자
프루네리, 발레리오
스페인, (바르셀로나) 카스텔데펠스 08860, 넘. 3, 에이브이. 칼 프리드리히 가우스, 파끄 메디테라니오 데 라 테크놀로지아, 푼다시오 인스티튜트 드 시엔시스 포토닉스
아벨란, 카를로스
스페인, (바르셀로나) 카스텔데펠스 08860, 넘. 3, 에이브이. 칼 프리드리히 가우스, 파끄 메디테라니오 데 라 테크놀로지아
(뒷면에 계속)
(74) 대리인
특허법인 무한

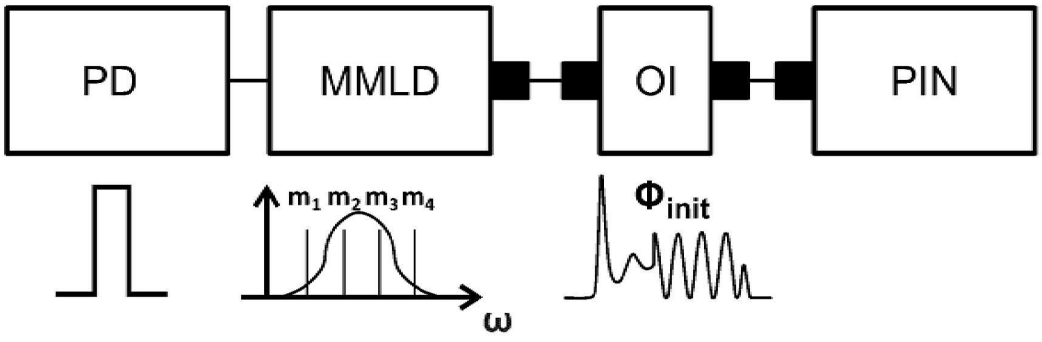
전체 청구항 수 : 총 4 항 심사관 : 지정훈

(54) 발명의 명칭 **다모드 레이저 캐비티 내 양자 난수 발생 프로세스**

(57) 요 약

본 발명은 전기 펄스 드라이버에 의해 이득-스위칭 메카니즘 하에서 다모드 레이저를 작동시키는 단계, 및 레이저 캐비티 내에서 발생하는 모드-간 비팅에 의해 생성되는 랜덤 강도 패턴을 검출하는 단계를 포함하는 양자 난수 발생기에 의해 난수를 생성하는 프로세스 및 시스템에 기초한다. 생성되는 수는 진성 랜덤(truly random)이고 최소한의 요소가 시스템 작동에 대해 필요하다

대 표 도 - 도1



(52) CPC특허분류
H01S 3/1106 (2023.01)
H01S 5/06213 (2013.01)
H01S 5/0623 (2013.01)
H01S 5/0652 (2013.01)
H01S 5/0657 (2013.01)
H01S 5/3013 (2013.01)
G06F 2207/58 (2013.01)
(72) 발명자
아마야, 발디마르
스페인, (바르셀로나) 카스텔데펠스 08860, 넘. 3, 에이브이. 칼 프리드리히 가우스, 파끄 메디테라니오 데 라 테크놀로지아, 푼다시오 인스티튜트 드 시엔시스 포토닉스
미첼, 모르간, 윌프레드
스페인, (바르셀로나) 카스텔데펠스 08860, 넘. 3, 에이브이. 칼 프리드리히 가우스, 파끄 메디테라니오 데 라 테크놀로지아, 푼다시오 인스티튜트 드 시엔시스 포토닉스

명 세 서

청구범위

청구항 1

양자 난수 발생기에 의해 난수를 생성하는 프로세스에 있어서,

a) 양수를 음수로 그리고 음수를 양수로 순 이득을 연속적으로 변조하는 전기 펄스 드라이버(PD)에 의해, 높은 변조 대역폭 및 깊이로 다모드 레이저 다이오드(MMLD)를 작동시키는 단계;

b) 캐비티의 왕복 시간보다 더 긴 기간 동안 왕복 당 상기 순 이득을 양수로 유지하는 단계;

c) 상기 캐비티의 상기 왕복 시간보다 더 긴 기간 동안 왕복 당 시간 순 이득을 음수로 유지하는 단계;

d) 고속 포토다이오드(PIN)에 의해 a)에서의 다중 모드들 간 결과 랜덤 비팅 패턴(resulting random beating pattern)을 검출하는 단계;

e) 후속 펄스를 샘플링하여 난수를 획득하는 단계

를 포함하는 프로세스.

청구항 2

제1항에 있어서,

비팅 프로세스(beating process)에 연관된 모드들의 개수를 감소시키기 위하여, 레이저 캐비티 내의 주파수들의 개수를 선택하는 단계

를 더 포함하는 프로세스.

청구항 3

제1항에 있어서,

상기 레이저는 비-공진 주파수에서 작동되어, 상기 캐비티의 종측 모드들 간 잠금 메카니즘이 방지되는

프로세스.

청구항 4

제1항 내지 제3항 중 어느 한 항에 있어서,

레이저 캐비티로의 반사되는 광 파워를 회피하기 위하여, 신호들을 광학적으로 아이솔레이팅(isolating)하는 단계

를 더 포함하는 프로세스.

발명의 설명

기 술 분 야

본 발명은 난수 발생기(random number generators)(RNGs)에 관한 것으로서, 특히 가변 이득 또는 손실(variable gain or loss)을 가지는 다모드 레이저 캐비티(multimode laser cavities) 내에서 양자 관측 값(quantum observables)의 고유 무작위성(intrinsic randomness)에 기초하는 생성기(generators)에 관한

것이다.

배 경 기 술

임의의 패턴이 없는 숫자 또는 기호의 시퀀스로부터의 난수(random numbers)는 임의적으로 나타난다. 난수 발생기(RNG)는 난수를 생성하도록 설계되는 계산 또는 물리적 장치(computational or physical device)이다. RNG는 의사-RNG (pseudo-RNGs)(PRNGs), 계산 알고리즘 및 트루-RNG(true-RNGs)(TRNGs)로 분류될 수 있다. TRNG는 물리적 장치이고 고전적인 결정론적 법칙(classical deterministic laws)을 기초로 하는 고전적인 RNG(classical RNGs)(CRNGs), 및 양자 효과(quantum effects)를 기초로 하는 양자 RNG(quantum RNGs)(QRNGs)로 세분화될 수 있다.

현재의 상용 RNG 장치(commercial RNG devices)는 많은 다른 방식 중에서(among many other schemes), 단일 광자의 공간 분포(spatial distribution of single photons) [1], 반도체 레이저의 카오스 이론(chaotic dynamics in semiconductor lasers) [2], CMOS 준안정성(metastability) [3], 단일 광자 검출기의 배열 내의 단일 광자 검출(single photon detection in arrays of single photon detectors) [4] 또는 반도체 레이저 내의 위상 확산(phase diffusion in semiconductor lasers) [5, 6]을 기초로 한다.

프루네리(Pruneri) 등에 의한 특허 출원 "초고속 양자 난수 발생기 및 그 시스템(ultrafast quantum random number generator and system thereof)" [5]은 펄스화 단일-모드 반도체 레이저 내에서의 양자 위상 확산(quantum phase diffusion) 측정에 기초하는 QRNG를 개시한다. 레이저를 임계 값 아래에서 이상으로 변조함으로써, 거의 동일한 강도 및 완전히 랜덤화되는 위상을 가지는 광 펄스(optical pulses)가 생성된다. 외부 간섭계(external interferometer)를 사용함으로써, 랜덤 위상(random phases)이 랜덤 진폭(random amplitudes)으로 변환된다- PIN 검출기로써 디지털화될 수 있음. 하나의 레이저 소스(laser source) 및 간섭계 대신에, 2 개의 레이저 소스가 결합기(combiner)와 함께 사용될 수 있다. 이 기술은 초고속 작동 방식(ultrafast operation regimes)을 허용하고, 최근의 출판물은 최대 40-80 Gbps의 비트율(bitrates)을 나타낸다 [7,8]. 그러나, 방사 및 커플링 광학 내에서 스펙트럼적으로 매치되는 외부 간섭 요소 또는 2 개의 레이저의 필요성은 레이아웃을 복잡하게 만든다- 요소의 수, QRNG 장치의 전체 치수를 증가시키고, 및, 경우에 따라서 QRNG의 성능은 구성 요소의 안정성에 영향을 받는 것과 같음(the need of an external interferometric element or two lasers which are spectrally matched in emission and coupling optics complicates the layout as it increases the number of elements, the overall dimension of the QRNG device, and, in some cases the performance of the QRNG is affected by the stability of the components). 예를 들어, 두 개의 레이저의 경우 방사 파장 스펙트럼은 좁아져야 하며 (단일 모드), 시간에 따라 매치되고 유지되어야 하며, 이는 본질적인 불안정성 및 환경 변화로 인해 달성하기가 항상 쉬운 것은 아니다(in the case of the two lasers their emission wavelength spectra have to be narrow (single mode), matched and maintained over time and this is not always easy to achieve due to intrinsic instability and environmental changes). 따라서, 초소형 및 양자 기계적 엔트로피 특성(ultrafast and quantum mechanical entropy properties)을 유지하는 감소되는 치수(풋 프린트)를 가지는, 소형 폼 팩터 RNG 소스(smaller form factor RNG source)가 필요하다.

발명의 내용

해결하려는 과제

과제의 해결 수단

본 발명의 목적은 양자 난수 생성 프로세스 및 따라서 종래 기술의 한계를 극복하는 시스템을 제공하는 것이다. 본 발명은 다모드 레이저(multimode laser)의 모드들의 랜덤 위상을 고속 포토다이오드(fast photodiode)를 이용하여 검출(detected)될 수 있는 랜덤 강도 패턴(random intensity patterns)으로의 변환(transformation)에 기초한다. 이 목적을 위해, 본 발명은 전기 펄스 드라이버에 의해 양수를 음수로 그리고 음수로부터 양수로 왕복 당 순 이득이 연속적으로 변조되는 다모드 레이저 다이오드(a multimode laser whose net gain per round trip is modulated continuously from positive to negative values and viceversa by means of an electrical pulse driver)를 이용하는(utilizing) 단계, 캐비티의 왕복 시간보다 더 긴 기간 동안 왕복 당 순 이득을 양수로 유지(maintaining net gain per round trip positive for a longer period than the round trip time of the cavity)하는 단계, 상기 캐비티의 상기 왕복 시간보다 더 긴 기간 동안 왕복 당 상기 시간 순

이득을 음수로 유지하는 단계 및 고속 포토다이오드(PIN)를 이용하는 레이저 캐비티의 종측 모드들 간 상기 결과 비팅 패턴을 검출(maintaining net gain per round trip negative for a longer period than the round trip time of the cavity and detecting the resulting beating pattern between the longitudinal modes of the laser cavity utilizing a fast photodiode (PIN))하는 단계를 포함한다.

본 발명을 구현하기 위한 다모드 레이저의 많은 상이한 방식이 있다- 예를 들어, 적절한 파장 선택 반사기(wavelength selective reflectors)를 통해 다모드 응답이 수행되는 패브리 페로 캐비티 반도체 레이저(Fabry Perot cavity semiconductor laser) 또는 모드 선택을 위한 광섬유 브래그 그레이팅(fiber Bragg gratings) 및 이득 매체(gain medium)로서 반도체 광 증폭기(semiconductor optical amplifier)를 포함하는 광섬유 링 레이저(fiber ring laser). 적어도 2개의 모드들을 가지는 임의의 레이저 캐비티는 원칙적으로, 상기 적어도 2개의 모드들 중 적어도 하나의, 순 이득- 즉, 캐비티 내 이득 및 손실 간 차 -이 적절하게 변조 될 수 있는 한 적합하고, 특히 충분히 음수의 순 이득 값과, 이에 상응하는, 큰 위상 확산을 수행할 수 있다(Any laser cavity which has at least two modes is in principle suitable as long as the net gain, i.e. the difference between gain and loss in the cavity, of at least one of the at least two modes can be properly modulated, in particular to achieve sufficiently negative net gain values and, correspondingly, large phase diffusion).

순 이득을 변조하기 위해, 레이저 이득, 캐비티의 손실 또는, 대안적으로, 레이저 이득 및 캐비티 손실 모두는 변조될 수 있다. 각각의 변조 사이클(modulation cycle)에서, 레이저는 2 개의 안정되는 작업 체제를 경험한다(the laser experiences two stable working regimes): (i) 다모드 레이저의 상이한 종측 모드들이 주파수 간격 및 모드들 간 상대적인 위상들에 의해 특징화되는(characterized) 랜덤 강도 패턴을 생성할 수 있는, 임계 값 이상(above threshold), 및 (ii) 레이저 캐비티 필드(laser cavity field)가 자발적 방사 체제(spontaneous emission regime)- 다음 변조 사이클 동안 모드들 간 상대 위상을 이 방식으로 재설정 및 랜덤화함(resetting and randomising) - 내에서 작동하도록 가해지는(forced), 임계 값 이하(below threshold). 레이저를 임계 값 아래로 가져 와서 왕복 시간과 비교하여 충분히 긴 시간 동안 이러한 상태로 유지하지 못하게 하여 유도 방사 광자가 새로운 유도 방사 펄스 생성이 후속 펄스의 패턴 간 상관 관계를 도입하기 전에 캐비티를 벗어나게 한다(Not succeeding in bringing the laser below threshold and keeping it in such a condition for a time sufficiently long compared to the round trip time so that the stimulated emission photons leave the cavity before generating a new stimulated emission pulse would introduce correlations between the patterns of subsequent pulses).

본 발명 덕분에, 특히 집적 광 회로를 이용하여 이를 구성 시, 매우 컴팩트한 (작은 풋프린트) 시스템을 이용하여, 임의의 외부 또는 간섭계 요소 없이 양자 수를 제공할 수 있다.

본 발명의 보다 양호한 이해를 위한 설명을 완성하기 위해, 일련의 도면이 제공된다. 상기 도면은 본 발명의 바람직한 실시 예를 도시하며, 본 발명의 범위를 제한하는 것으로 해석되어서는 안되며, 본 발명이 어떻게 구현될 수 있는지의 예로서 해석되어야 한다.

도면의 간단한 설명

도 1은 본 발명을 실시하기 위한 가능한 구성을 도시한다.

도 2는 다른 구성을 도시한다.

도 3은 다-모드 레이저(multi-mode laser)의 두 가지 작동 영역(에 대한 자기 상관 함수(autocorrelation function)를 도시한다.

발명을 실시하기 위한 구체적인 내용

도 1은 다모드 레이저 다이오드(multimode laser diode)(MMLD)의 캐비티 내에서 선택적 필터링을 통해 2-모드 레이저(two-mode laser)가 획득되는, 본 발명을 실시하기 위한 제1 설정을 도시한다. MMLD는 전기 펄스 드라이버(electrical pulse driver)(PD)를 통해 변조된다. 예에서 두 가지 모드만 선택되었으므로, 포토다이오드(photodiode)(PIN)를 이용하여 검출될 때 비팅 패턴은 모드 간격 (도에서 모드 m2 및 m3 사이의 주파수 차)에 의해 주어지는 주파수와 특정 기간 내의 모드들 간 위상 차에 의해 주어지는 초기 위상 Φ_{init}을 가지는 코사인 의존성을 보여준다(Since only two modes are selected in the example, the beating pattern when detected with the photodiode (PIN) shows cosine dependence with a frequency given by the mode spacing

(frequency difference between modes m2 and m3 in the figure) and initial phase Φ_{init} given by the phase difference between the modes in that particular period). 레이저 캐비티로의 광학 백 반사(optical back reflections)를 피하기 위해 광학 아이솔레이터(optical isolator)(OI)가 추가될 수 있다.

결과 강도 패턴(resulting intensity pattern)은 랜덤 초기 위상(random initial phase)을 가지는, 이중-모드 방사(dual-mode emission)로 인한, 코사인 의존성(cosine dependence)을 보여준다. 따라서, 유효 레이저 캐비티 이득(effective laser cavity gain)을 변조함으로써 생성되는 각각의 펄스는 2 개의 모드들의 랜덤 초기 위상 상에 구축되기 때문에, 후속 펄스 샘플링은 랜덤 진폭의 디지털화(digitization)를 생성한다. 비팅에 연관되는 모드들의 수가 클수록, 결과 강도 패턴은 더 복잡해지고 각 순 이득 변조 사이클 내에서 추출될 수 있는 랜덤 샘플의 수가 더 커진다.

시스템이 양자 랜덤 샘플(숫자)을 제공하는 시스템에 대해 레이저 캐비티의 순 이득 변조는 필수적임을 유의해야 한다. 순 이득이 임계 값(threshold) 이상으로 일정하게 유지되면, 모드 비팅(mode beating)은 여전히 존재하지만 캐비티를 떠나는 펄스 사이에서 상관 관계(correlations)가 존재할 수 있다. 순 이득이 캐비티의 왕복과 연관되는 주파수로 변조되는 경우, 이 모드 비팅은 주기적 펄스의 열(a train of periodic pulses)을 생성하는 모드-잠금(mode-locking)으로 알려진 것이 될 수 있다.

통합되는 버전의 구조에 대한 유사한 구조는 다음과 같이 될 수 있다: 활성 물질(active material)을 광자 집적 회로(photonic integrated circuit)(PIC) 내부 또는 상부에 배치시킴, 및 칩(chip) 자체의 쪼개진 면(cleaved facets)을 미러(mirrors)로서 사용. 스펙트럼 필터링(spectral filtering)은 활성 물질의 양면 상에 그레이팅(gratings)를 배치하거나, 또는 고리-같은(ring-like) 구조를 사용함으로써 수행될 수 있다.

도 2에서, 인화인듐(InP) 또는 인듐 갈륨 비소 인화물(InGaAsP)와 같은 활성 물질은 고 반사성 엔드 미러(highly reflective end mirrors)를 가지는 패브리 페로 캐비티(Fabry Perot cavity) 내에 배치된다. 미러의 스펙트럼 반사율(spectral reflectivity)은 캐비티 자체가 약간의 모드들만 발진(oscillate)하도록 하는 필터(filter)로서 역할을 하도록 설계될 수 있다. 도 2a에서, 2 개의 반사 미러는 2 개의 원하는 모드들(CRC1,2)을 필터링할 수 있다. 활성 매체(active medium)를 전기적으로 펌핑함(electrically pumping)으로써 레이징(lasing)이 발생할 수 있고 브로드 다모드 광 스펙트럼(broad multimode optical spectrum)이 생성된다. 미러들 간의 분리와 그 사이의 물질의 굴절률(The separation between the mirrors and the refractive index of the material in between)은 모드 간격(mode spacing)을 결정한다. 최종적으로, 모드 간격이 검출 대역폭보다 작도록 캐비티가 설계되면, 레이저의 모드-간 비팅(inter-mode beating)은 고속 포토다이오드(PIN)로써 해결될 수 있다.

도 2b에서, 활성 물질(active material)은 포토닉 칩의 상부에 배치되고(deposited), 칩의 쪼개진 면에 의해 생성되는 반사를 사용하여 캐비티가 생성된다. 스펙트럼 필터링(spectral filtering)은 그레이팅에 의해 획득된다.

도 3은 2 개의 작동 영역에 대한 자기 상관 함수를 도시한다: (상단 그림) 레이저가 자발 방사 영역(spontaneous emission regime)에 도달하지 못하고, (하단 그림) 레이저가 자발 방사 영역에 성공적으로 도달함. 상단 그림에서, 레이저는 자발 방사 영역에 도달하지 않으므로, 상관 관계 함수(correlation function)는 후속 펄스들(subsequent pulses) 간 패턴들이 유사함을 개시한다(그림 내에 피크(peaks)로서 도시됨). 대신에, 하단 그림에서, 후속 펄스 간 위상의 완전한 랜덤화(complete randomization of the phase)로 인한 상관 관계는 관찰되지 않는다.

본 명세서에서, 용어 "포함함(comprises)"및 그 파생 ("포함하는(comprising)"과 같음)은 배타적인 의미로 이해되어서는 안되며, 즉, 이 용어들은 기술되고 정의되는 것이 추가 요소, 단계 등을 포함할 수 있는 가능성을 배제하는 것으로 해석되어서는 안된다.

한편, 본 발명은 분명히 본 명세서에 기술되는 특정 실시 예(들)에 한정되지 않고, 당업자에 의해 고려될 수 있는 임의의 변형을 또한 포괄한다(예를 들어, 선택 구성 요소, 구성 등과 연관함)- 청구 범위 내에서 정의되는 본 발명의 일반적인 범위 내에서.

참조(References)

[1] G. Ribordy et al, "Method and apparatus for generating true random numbers by way of a quantum optics process", US 7519641 B2 (2009).

[2] A. Uchida et al, "Fast physical random bit generation with chaotic semiconductor lasers", Nat. Photonics, vol. 2, 12, 728-732 (2008)

[3]H.C. Herbert et al, "Digital random number generator", US20100332574A1 (2010)

[4] S. Tisa et al, "High-Speed Quantum Random Number Generation Using CMOS Photon Counting Detectors", IEEE Journal of Selected Topics in Quantum Electronics, (21) 3, 23-29 (2015)

[5] V. Pruneri et al, "Ultrafast quantum random number generation process and system therefor", US2013/0036145 A1

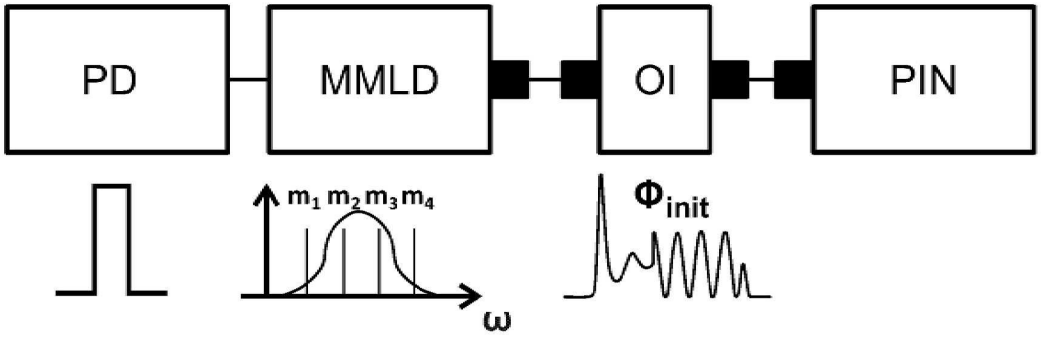
[6] F. Xu et al, "An ultrafast quantum random number generator based on quantum phase fluctuations", Opt. Express 20, 12366 (2012)

[7] Z.L. Yuan et al, "Robust random number generation using steady-state emission of gain-switched laser diodes", Appl. Phys. Lett. 104, 261112 (2014)

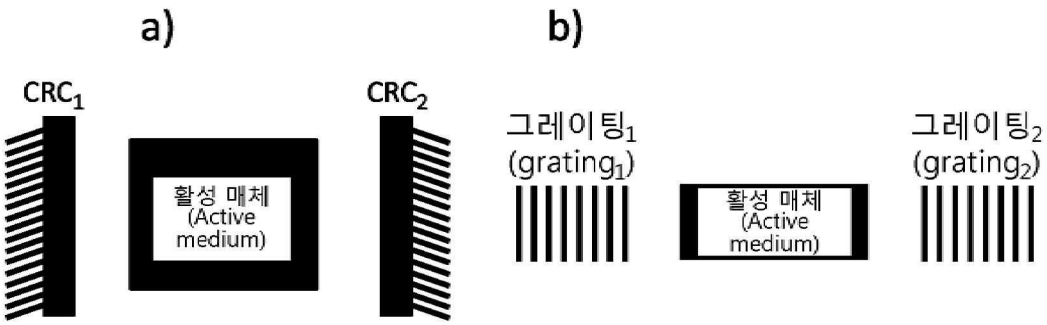
[8] C. Abellan et al, "Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode", Opt. Express 22, 1645 (2014)

도면

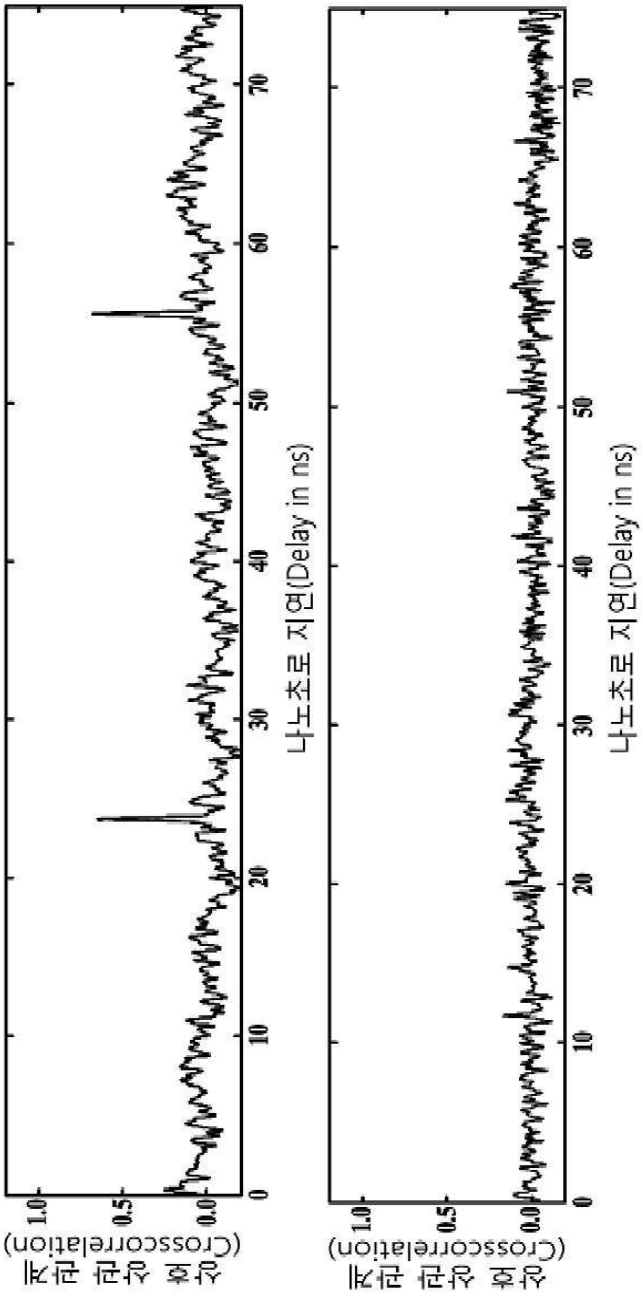
도면1



도면2



도면3


상호 상관 관계
(Crosscorrelation)
1.0
0.5
0.0
0
10
20
30
40
50
60
70
나노초로 지연(Delay in ns)
상호 상관 관계
(Crosscorrelation)
1.0
0.5
0.0
0
10
20
30
40
50
60
70
나노초로 지연(Delay in ns)