(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2021년08월12일
(11) 등록번호 10-2289084
(24) 등록일자 2021년08월06일

(51) 국제특허분류(Int. Cl.)
G06F 7/58 (2006.01) *G06F 15/78* (2006.01)
(52) CPC특허분류
G06F 7/588 (2013.01)
G06F 15/7803 (2013.01)
(21) 출원번호 10-2021-7021472
(22) 출원일자(국제) 2020년12월18일
심사청구일자 2021년07월08일
(85) 번역문제출일자 2021년07월08일
(86) 국제출원번호 PCT/US2020/065976
(87) 국제공개번호 WO 2021/097468
국제공개일자 2021년05월20일
(30) 우선권주장
63/062,672 2020년08월07일 미국(US)
(뒷면에 계속)
(56) 선행기술조사문헌
KR1020180035223 A
KR1020190055179 A

(73) 특허권자
란데몬 에스피. 제트 오.오.
폴란드 바르샤바 02-858 유엘. 크사웨로우 21
(72) 발명자
타타르키위츠, 잔, 제이.
미국 캘리포니아 92130-1528 샌디에이고 유닛 170 시그니처 포인트 13029
쿠즈미츠, 와이스로우, 보단
폴란드 바르샤바 02-785 유엘. 푸스치카 18에이 엠.
보로드진스키, 자누스, 저지
폴란드 바르샤바 01-117 고르체우스카 90
(74) 대리인
김정훈

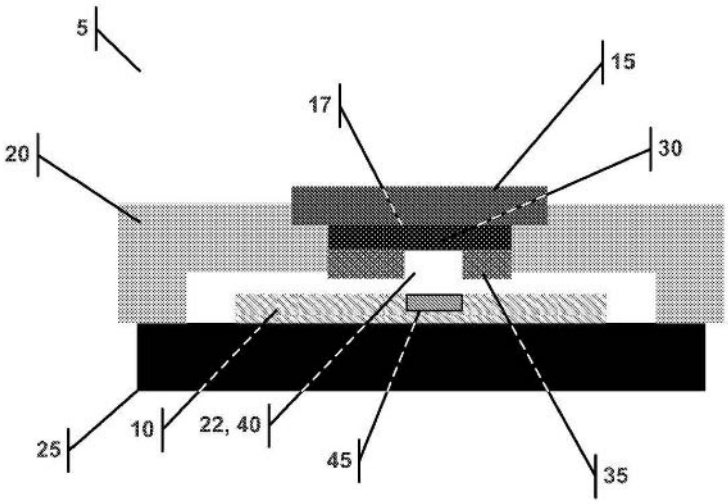
전체 청구항 수 : 총 26 항 심사관 : 지정훈

(54) 발명의 명칭 **베타 붕괴 기반의 진성 난수 생성기를 위한 장치, 시스템, 및 방법**

(57) 요 약

본 명세서에는 진성 난수 생성기(TRNG)가 개시된다. TRNG는 공동을 획정하는 인클로저 및 공동을 덮으며 공동에 노출된 캡 표면을 갖는 캡을 포함하고, 캡 표면은 방사성 니켈을 포함한다. 공동 내의 전자 센서는 니켈의 붕괴로부터의 전자들을 검출하며 검출된 에너지에 대한 신호를 생성한다. 증폭기는 센서에 연결되어 신호를 증폭하도록 구성되며 신호를 필터에 공급한다. 필터에 연결된 프로세서는 신호에 기초하여 진성 난수를 생성한다. 이 TRNG는 집적 회로 상에 형성될 수 있다.

대 표 도 - 도1d



(30) 우선권주장
62/984,528 2020년03월03일 미국(US)
16/990,087 2020년08월11일 미국(US)

명 세 서

청구범위

청구항 1

진성 난수 생성기(true random number generator: TRNG)로서,

집적 회로(integrated circuit: IC)의 표면 위에 공동(cavity)을 획정하는 인클로저; 상기 공동에 노출된 캡 표면 - 상기 캡 표면은 방사성 니켈을 포함함 - 으로 상기 공동을 덮는 캡; 상기 방사성 니켈의 일부의 위에 적용되며 상기 방사성 니켈에 의해 상기 공동 내로 방출되는 전자들의 양과 방향을 제한하도록 구성된 마스크를 포함하고;

상기 IC는: 상기 캡 표면으로부터 상기 공동의 건너편에 소정 거리에 위치된 전자 센서 - 상기 전자 센서는 상기 공동 내의 상기 방사성 니켈에 의해 방출되는 전자들을 검출하고 상기 검출된 전자들에 대한 신호를 발생시키도록 상기 마스크의 보이드(void)와 정렬되도록 구성됨 -; 상기 전자 센서에 연결되고 상기 신호를 증폭하도록 구성된 증폭기; 상기 신호를 필터링하도록 구성된 상기 증폭기에 연결된 필터; 상기 필터에 연결된 프로세서 - 상기 프로세서는 상기 신호를 기초로 진성 난수를 생성하도록 구성됨 - 를 포함하며;

상기 마스크는 상기 방사성 니켈에 의해 방출되는 전자들로부터 상기 증폭기, 필터, 및 프로세서를 적어도 부분적으로 차폐하는,

TRNG.

청구항 2

제1 항에 있어서,

상기 프로세서는 다음의 단계들: a. 상기 신호가 니켈의 붕괴 이벤트들을 나타내는지 여부를 결정하는 단계; b. 붕괴 이벤트들 사이의 기간을 결정하기 위해 타이머를 설정하는 단계; c. 단계 (b)의 기간들에 기초하여 0 또는 1의 값을 할당하는 단계; d. 상기 값을 메모리에 저장하는 단계; e. 단계 (b) - (d)를 반복하여 값들의 스트링(string)을 산출하는 단계; 및 f. 상기 값들의 스트링을 기초로 진성 난수를 생성하는 단계를 수행하도록 구성되는,

TRNG.

청구항 3

제2 항에 있어서,

단계 (b)는: 제1 쌍의 붕괴 이벤트 사이의 제1 기간 T1; 제2 쌍의 붕괴 이벤트 사이의 제2 기간 T2를 결정하는 단계를 더 포함하고; 단계 (c)는 T1과 T2를 비교하는 단계 및 상기 비교에 기초하여 상기 값을 할당하는 단계를 더 포함하는,

TRNG.

청구항 4

제3 항에 있어서,

상기 제1 쌍의 붕괴 이벤트와 상기 제2 쌍의 붕괴 이벤트는 공통의 붕괴 이벤트를 공유하는,

TRNG.

청구항 5

제1 항에 있어서,

상기 마스크는 적어도 100 미크론의 두께이며 100 keV 미만의 에너지를 갖는 전자들을 흡수하는,

TRNG.

청구항 6

제1 항에 있어서,

상기 프로세서는 진성 난수들의 어레이를 생성하는,

TRNG.

청구항 7

제6 항에 있어서,

상기 프로세서는 상기 진성 난수들의 어레이를 암호화 클라이언트에 제공하며; 전달된 진성 난수를 메모리에서 삭제하는,

TRNG.

청구항 8

제7 항에 있어서,

상기 제공된 진성 난수의 어레이는 상기 어레이에서 가장 오래된 것인,

TRNG.

청구항 9

제6 항에 있어서,

메모리가 가득 차면, 상기 프로세서는 상기 진성 난수들의 어레이에서 가장 오래된 것을 삭제하는,

TRNG.

청구항 10

제1 항에 있어서,

상기 진성 난수는 256 비트 또는 512 비트로 구성되는,

TRNG.

청구항 11

제1 항에 있어서,

상기 방사성 니켈은 적어도 초당 100 만 개의 붕괴 이벤트를 발생시키기에 충분한 양인,

TRNG.

청구항 12

제1 항에 있어서,

적어도 1 GHz의 클럭 주파수를 갖는 타이머를 포함하는, TRNG.

청구항 13

제1 항에 있어서,

상기 증폭기는 저노이즈의 전하에 민감한 전치 증폭기 또는 펄스 성형 증폭기를 포함하는,

TRNG.

청구항 14

제1 항에 있어서,

상기 전자 센서는 센서 어레이인,

TRNG.

청구항 15

제14 항에 있어서,

상기 프로세서는 다음의 단계들: a. 상기 어레이 내의 센서들 각각으로부터의 검출에 기초하여 0 또는 1을 할당하는 단계; b. 단계 (a)를 기초로 진성 난수들의 어레이를 생성하는 단계를 수행하도록 구성되는,

TRNG.

청구항 16

제15 항에 있어서,

상기 프로세서는 다음의 엔트로피 조정 하위단계들: c. 상기 센서 어레이의 판독 속도(reading rate)를 설정하는 단계; d. 상기 센서 어레이에 의해 리포팅되는 0의 개수와 상기 센서 어레이에 의해 리포팅되는 1의 개수를 비교하는 단계; e. 단계 (d)에서의 상기 비교에 기초하여 상기 판독 속도를 조정하는 단계를 수행하도록 구성되는,

TRNG.

청구항 17

진성 난수 생성기로서, 집적 회로(integrated circuit: IC)의 표면 위에 공동을 획정하는 인클로저; 상기 공동에 노출된 캡 표면 - 상기 캡 표면은 방사성 니켈을 포함함 - 으로 상기 공동을 덮는 캡; 상기 방사성 니켈의 일부의 위에 적용되며 상기 방사성 니켈에 의해 상기 공동 내로 방출되는 전자들의 양과 방향을 제한하도록 구성된 마스크를 포함하고; 상기 IC는: 상기 캡 표면으로부터 상기 공동의 건너편에 소정 거리에 위치된 전자 센서 - 상기 전자 센서는 상기 공동 내의 상기 방사성 니켈에 의해 방출되는 전자들을 검출하고 상기 검출된 전자들에 대한 신호를 발생시키도록 상기 마스크의 보이드와 정렬되도록 구성됨 -; 상기 전자 센서에 연결되고 상기 신호를 증폭하도록 구성된 증폭기; 상기 신호를 필터링하도록 구성된 상기 증폭기에 연결된 필터; 상기 필터에 연결된 프로세서 - 상기 프로세서는 상기 신호를 기초로 진성 난수를 생성하도록 구성됨 - 를 포함하며; 상기 마스크는 상기 방사성 니켈에 의해 방출되는 전자들로부터 상기 증폭기, 필터, 및 프로세서를 적어도 부분적으로 차폐하는, 상기 진성 난수 생성기; 및

상기 진성 난수를 수신하도록 적합화된 암호화 클라이언트:

를 포함하는, 개인용 전자 디바이스.

청구항 18

제17 항에 있어서,

상기 진성 난수는 통신 채널을 암호화하거나, 컴퓨터 시뮬레이션들을 렌더링하거나, 또는 컴퓨터 게이밍을 렌더링하는 데 사용되는,

개인용 전자 디바이스.

청구항 19

제17 항에 있어서,

상기 마스크는 적어도 100 미크론의 두께이며 100 keV 미만의 에너지를 갖는 전자들을 흡수하는,

개인용 전자 디바이스.

청구항 20

방사성 니켈과 전자 센서를 사용하여 진성 난수를 생성하는 방법으로서,

a. 소정량의 방사성 니켈에 상기 전자 센서를 노출시키는 단계; b. 상기 전자 센서와 상기 소정량의 방사성 니켈 사이에 배치된 마스크로 상기 전자 센서의 노출을 포커싱하는 단계; c. 상기 전자 센서에 의해 상기 방사성 니켈의 붕괴로부터의 전자 신호를 검출하는 단계; d. 상기 전자 신호가 방사성 니켈의 붕괴 이벤트들을 나타내는지 여부를 결정하는 단계; e. 붕괴 이벤트들 사이의 기간을 결정하기 위해 타이머를 설정하는 단계; f. 상기 기간을 기초로 0 또는 1의 값을 할당하는 단계; g. 상기 값을 저장하는 단계; h. 단계 (c) - (g)를 반복하여 값들의 스트링을 산출하는 단계; 및 i. 상기 값들의 스트링을 기초로 진성 난수들의 어레이를 생성하는 단계:

를 포함하는, 방법.

청구항 21

제20 항에 있어서,

단계 (e)는: 제1 쌍의 붕괴 이벤트 사이의 제1 기간 T1; 제2 쌍의 붕괴 이벤트 사이의 제2 기간 T2를 결정하는 단계를 더 포함하고; 단계 (f)는 T1과 T2를 비교하는 단계 및 상기 비교에 기초하여 상기 값을 할당하는 단계를 더 포함하는,

방법.

청구항 22

제21 항에 있어서,

상기 제1 쌍의 붕괴 이벤트와 상기 제2 쌍의 붕괴 이벤트는 공통의 붕괴 이벤트를 공유하는,

방법.

청구항 23

제20 항에 있어서,

j. 상기 진성 난수들의 어레이를 암호화 클라이언트에 제공하는 단계; 및 k. 상기 제공된 진성 난수들의 어레이를 삭제하는 단계:

를 더 포함하는, 방법.

청구항 24

제20 항에 있어서,

상기 진성 난수는 256 비트 또는 512 비트로 구성되는,

방법.

청구항 25

방사성 니켈과 전자 센서 어레이를 사용하여 진성 난수를 생성하는 방법으로서,

a. 소정량의 방사성 니켈에 상기 전자 센서 어레이를 노출시키는 단계; b. 상기 전자 센서 어레이와 상기 소정량의 방사성 니켈 사이에 배치된 마스크로 상기 전자 센서 어레이의 노출을 포커싱하는 단계; c. 상기 전자 센서 어레이에 의해 판독 속도(reading rate)로 상기 방사성 니켈의 붕괴로부터의 전자 신호를 검출하는 단계; d. 상기 전자 신호가 방사성 니켈의 붕괴 이벤트들을 나타내는지 여부를 결정하는 단계; e. 상기 어레이 내의 각 전자 센서로부터의 검출에 기초하여 0 또는 1을 할당하는 단계; 및 f. 단계 (e)에 기초하여 진성 난수들의 어레이를 생성하는 단계:

를 포함하는, 방법.

청구항 26

제25 항에 있어서,

g. 단계 (f)에서 상기 전자 센서 어레이에 의해 할당되는 0의 개수와 상기 전자 센서 어레이에 의해 할당되는 1의 개수를 비교하는 단계; 및 h. 단계 (g)에서의 상기 비교에 기초하여 상기 판독 속도를 조정하는 단계:

를 포함하는 엔트로피 조정 하위방법을 더 포함하는, 방법.

청구항 27

삭제

청구항 28

삭제

발명의 설명

기 술 분 야

[0001] 기술 분야

[0002] 본 발명은 일반적으로 진성 난수 생성기, 구체적으로는 자발적 니켈 동위원소 붕괴를 이용한 난수 생성기 기술, 및 이에 관한 장치, 시스템, 및 방법에 관한 것이다.

[0003] 우선권 출원

[0004] 본 출원은 발명의 명칭이 "트리튬 기반의 진성 난수 생성기를 위한 방법 및 장치"인 2020년 3월 3일자로 제출된 미국 가출원 SN 제62/984,528호, 및 발명의 명칭이 "베타 붕괴 기반의 진성 난수 생성기를 위한 방법 및 장치"인 2020년 8월 7일자로 제출된 미국 가출원 SN 제63/062,672호의 우선권을 주장한다.

[0005] 본 출원은 발명의 명칭이 "트리튬 난수 생성기를 포함하는 장치, 시스템, 및 방법"인 2018년 4월 9일자로 제출된 미국 가출원 SN 제62/655,172호, 발명의 명칭이 "트리튬 난수 생성기를 포함하는 장치, 시스템, 및 방법"인 2019년 2월 9일자로 제출된 미국 가출원 SN 제62/803,476호, 및 발명의 명칭이 "트리튬 난수 생성기를 포함하는 장치, 시스템, 및 방법"인 2019년 2월 12일자로 제출된 미국 출원 SN 제16/273,365호 - 현재는 미국 특허 제10,430,161호임 - 에도 또한 관련된다.

[0006] 본 명세서에서 논의 및/또는 인용된 특허 출원들, 허여된 특허들, 및 기타 참고 문헌들 각각은 마치 본 명세서에 전체가 기재된 것처럼 참조로 편입되어 있다.

배 경 기 술

[0007] 수치 알고리즘들에 기초한 의사(pseudo) 난수 생성기와 대조적으로, 자연적인 랜덤 프로세스들: 복수의 바이폴라 스위치, 열 잡음, 다이크로익 미러들(dichroic mirrors)에 의한 광 산란, 카오스 시스템들, 방사성 원자핵들의 붕괴에 의존하는 진성 난수 생성기(true random number generator: TRNG) 디바이스들이 있다. 이들 TRNG 중 몇 가지는 본 출원이 우선권을 주장하는 가출원들에 나열되어 있으며, 이들 참고 문헌들은 마치 본 명세서에 전체가 기재된 것처럼 참조로 본 명세서에 편입되어 있다.

[0008] 방사성 핵종의 붕괴는 온도, 압력, 또는 가속도와 같은 환경적 영향들에 가장 독립적인 것으로 여겨진다. 하지만, 전형적인 원자핵 기반의 TRNG들은 방사성 붕괴의 결과로 방출되는 입자들의 등록을 가능하게 하기 위해 대형 검출기들을 필요로 한다. 또한, 이러한 디바이스들에 사용되는 많은 원자핵은 고도로 방사성 및 유독성이며, 그래서 디바이스가 손상되면 인간에게 위험하다.

발명의 내용

해결하려는 과제

[0009] 따라서, 사용자를 위험한 수준의 방사선에 노출시키지 않는 안전하고 소형인 TRNG가 유리하다 할 것이다. 이러한 TRNG는 그러면 컴팩트한 개인용 디바이스들에 사용될 수 있다.

과제의 해결 수단

[0010] 본 명세서에 개시된 발명은 진성 난수 생성기(true random number generator: TRNG)이다. TRNG는 공동(cavity)을 획정하는 인클로저 및 공동을 덮으며 공동에 노출된 캡 표면을 갖는 캡을 포함하고, 캡 표면은 방사성 니켈을 포함한다. 전자 센서는 니켈의 붕괴로부터의 공동 내의 전자들을 검출하며 검출된 에너지에 대한 신

호를 생성한다. 증폭기는 센서에 연결되어 신호를 증폭하도록 구성되며 신호를 필터에 공급한다. 필터에 연결된 프로세서는 신호에 기초하여 진성 난수를 생성한다. 진성 난수는 256 비트, 512 비트, 또는 적용에서 요구하는 다른 비트 수로 구성될 수 있다.

[0011] 프로세서는 다음의 단계들을 수행하도록 구성될 수 있다: (a) 신호가 니켈의 붕괴 이벤트들을 나타내는지 여부를 결정하는 단계; (b) 여러 붕괴 이벤트 사이의 기간을 결정하기 위해 타이머를 설정하는 단계; (c) 단계 (b)의 기간들에 기초하여, 0 또는 1의 값을 할당하는 단계; (d) 값을 메모리에 저장하는 단계; (e) 단계 (b) - (d)를 반복하여 값들의 스트링(string)을 산출하는 단계; 및 (f) 값들의 스트링을 기초로 진성 난수를 생성하는 단계. 단계 (b)는 제1 쌍의 붕괴 이벤트 사이의 제1 기간 T1 및 제2 쌍의 붕괴 이벤트 사이의 제2 기간 T2를 결정하는 단계를 더 포함할 수 있다. 그리고 단계 (c)는 T1과 T2를 비교하고는 시간 길이들의 비교에 기초하여 값을 할당한다. 제1 쌍의 붕괴 이벤트와 제2 쌍의 붕괴 이벤트는 공통의 붕괴 이벤트를 공유할 수 있다. 프로세서는 진성 난수들의 어레이를 생성할 수 있고, 어레이를 암호화 클라이언트에 제공하며 그리고 나서 전달된 진성 난수를 메모리에서 삭제할 수 있다.

[0012] 공동, 센서, 증폭기, 필터, 및 프로세서는 집적 회로(IC)에 형성된다. 니켈은 캡 상에 니켈을 염 전기도금(salt electroplating)한 결과일 수 있다. 니켈의 양은 바람직하게는 적어도 초당 100 만 개의 붕괴 이벤트를 발생시키기에 충분하다. TNRG는 적어도 1 GHz의 클럭 주파수를 갖는 타이머를 포함할 수 있다. 증폭기는 저노이즈의 전하에 민감한 전치 증폭기 또는 펄스 성형 증폭기일 수 있다.

[0013] 전자 센서는 센서 어레이일 수 있으며, 프로세서는 다음의 단계들: (a) 어레이 내의 몇몇 센서(픽셀)에 의한 전자들의 검출에 기초하여 0 또는 1(0은 검출 없음에 대응하는 한편 1은 적어도 하나의 전자의 검출에 대응함)을 할당하는 단계; 및 (b) 아래의 단계 (d)를 기초로 진성 난수들의 어레이를 생성하는 단계를 수행할 수 있다. 프로세서는 다음의 엔트로피 조정 하위단계들를 수행할 수 있다: (c) 센서들의 판독 속도(reading rate)를 설정하는 단계; (d) 센서 어레이에 의해 리포팅되는 0의 개수와 센서 어레이에 의해 리포팅되는 1의 개수를 비교하는 단계; 및 (e) 통계 오차 내에서 0과 1의 개수가 같도록 단계 (d)에서의 비교에 기초하여 판독 속도를 조정하는 단계.

[0014] 본 기술분야의 통상의 기술자에게 명백한 추가적인 양태들, 대체물들, 및 변경들도 본 명세서에 개시되며 본 발명의 일부로서 포함되는 것으로 구체적으로 고려된다. 본 발명은 본 출원 또는 관련 출원들에서 특허청이 허여하는 청구범위에만 명시되며, 이하의 특정 예들의 개요 설명은 어떠한 방식으로도 법적 보호의 범위를 제한, 규정, 또는 확립하지 않는다.

도면의 간단한 설명

[0015] 다음의 도면들을 참조하면 본 발명이 보다 잘 이해될 수 있다. 도면들 내의 컴포넌트들은 반드시 축척에 맞지는 않으며, 대신에 본 발명의 예시적인 양태들을 명확하게 도시하는 데 중점을 두고 있다. 도면들에서, 동일한 참조 번호들은 상이한 도면들 및/또는 실시예들에 걸쳐 대응하는 부분들을 나타낸다. 또한, 개시된 상이한 실시예들의 다양한 특징들은 본 발명의 일부인 추가 실시예들을 형성하도록 결합될 수 있다. 본 발명을 보다 명확하게 설명하는 것을 돕기 위해 특정 컴포넌트들 및 세부 사항들은 도면들에 나타나지 않을 수 있음을 이해할 것이다.

도 1a는 캡을 갖는 인클로저 내의 베타 붕괴 검출기의 단면도이다.

도 1b는 방사성 물질을 포함하는 캡을 갖는 베타 붕괴 검출기의 단면도이다.

도 1c는 방사성 물질을 포함하는 캡과 방사성 물질의 일부를 차폐하는 마스크를 갖는 베타 붕괴 검출기의 단면도이다.

도 1d는 완전히 조립된 베타 붕괴 검출기의 단면도이다.

도 2는 집적 회로에 배치될 수 있는 다양한 컴포넌트들의 흐름도이다.

도 3a는 랜덤 비트 스키마(random bit schema)당 4 개의 펄스를 도시한다.

도 3b는 랜덤 비트 스키마당 2 개의 펄스를 도시한다.

도 4는 어레이 기반의 검출기에 사용되는 엔트로피 조정 하위단계들/방법을 도시한다.

발명을 실시하기 위한 구체적인 내용

[0016] 여기서는 본 발명을 수행하기 위해 본 발명자에 의해 구상되는 임의의 최상의 모드를 포함하는 본 발명의 몇몇 구체적인 예에 대해 참조가 이루어진다. 이들 구체적인 실시예의 예들은 첨부된 도면들에 도시되어 있다. 본 발명이 이들 구체적인 실시예와 연계하여 설명되지만, 본 발명을 설명되거나 도시된 실시예들로 한정하려는 것이 아님을 이해할 것이다. 오히려, 첨부된 청구범위에 의해 정의되는 본 발명의 사상과 범위 내에 포함될 수 있는 대체물들, 변형들, 및 등가물들을 포함하도록 의도된다.

[0017] 이하의 설명에서는, 본 발명의 온전한 이해를 제공하기 위해 많은 구체적인 세부 사항이 명시된다. 본 발명의 특정의 예시적인 실시예들은 이들 구체적인 세부 사항의 일부 또는 전부 없이도 구현될 수 있다. 다른 경우들에는, 본 발명을 불필요하게 모호하게 하지 않기 위해 본 기술분야의 통상의 기술자에게 잘 알려진 프로세스 동작들은 상세하게 설명되지 않았다. 본 발명의 다양한 기법들 및 메커니즘들은 명확성을 위해 때로는 단수형으로 기재될 것이다. 하지만, 달리 언급되지 않는 한 몇몇 실시예는 기법의 복수 회의 반복 또는 복수의 메커니즘을 포함한다는 것에 유의해야 한다. 유사하게, 본 명세서에 도시되고 설명되는 방법들의 다양한 단계들은 반드시 나타낸 순서로 수행되는 것은 아니며, 또는 특정 실시예들에서는 전혀 수행되지 않는다. 따라서, 본 명세서에서 논의되는 방법들의 몇몇 구현예는 도시되거나 설명되는 것보다 더 많거나 적은 수의 단계를 포함할 수 있다. 또한, 본 발명의 기법들 및 메커니즘들은 때로는 2 개 이상의 엔티티 사이의 연결, 관계, 또는 통신을 기술하게 된다. 임의의 2 개의 엔티티 사이에는 다양한 다른 엔티티들 또는 프로세스들이 상주하거나 발생할 수 있으므로 엔티티들 사이의 연결 또는 관계가 반드시 직접적이며 방해받지 않는 연결을 의미하는 것은 아니라는 것에 유의해야 한다. 따라서, 달리 언급되지 않는 한 나타낸 연결은 반드시 직접적이며 방해받지 않는 연결을 의미하는 것은 아니다.

[0018] 다음의 예시적인 특징부들의 목록은 도 1 내지 도 4에 대응하며 참조의 편의를 위해 제공되는데, 동일한 참조 번호들은 명세서와 도면들 전체에 걸쳐 대응하는 특징부들을 지정한다.

[0019] 5: 검출기를 갖는 패키징된 집적 회로(IC)

[0020] 10: IC를 갖는 기판

[0021] 15: 캡

[0022] 17: 캡 표면

[0023] 20: IC 인클로저

[0024] 22: 공동(cavity)

[0025] 25: IC 베이스

[0026] 30: 방사성 물질

[0027] 35: 마스킹

[0028] 40: 마스킹 보이드(void)

[0029] 45: 방사성 검출기/센서

[0030] 210: 증폭기

[0031] 215: 필터

[0032] 220: 프로세서

[0033] 225: 신호 프로세서

[0034] 230: 타이머

[0035] 235: 메모리

[0036] 240: 암호화 클라이언트

[0037] 300: 검출기 어레이에 사용되는 방법

[0038] 수치 알고리즘들에 기초한 의사 난수 생성기와 대조적으로, 자연적인 랜덤 프로세스들: 복수의 바이폴라

스위치, 열 잡음, 다이크로익 미러들에 의한 광 산란, 카오스 시스템들, 방사성 원자핵들의 붕괴에 의존하는 많은 진성 난수 생성기(true random number generator: TRNG) 디바이스들이 있다. 후자의 그룹은 온도, 압력, 또는 가속도와 같은 환경적 영향들에 가장 독립적인 것으로 여겨진다. 하지만, 전형적인 원자핵 기반의 TRNG들은 방사성 붕괴의 결과로 방출되는 입자들의 등록을 가능하게 하기 위해 대형 검출기들을 필요로 한다. 또한, 이러한 디바이스들에 사용되는 많은 원자핵은 고도로 방사성 및 유독성이며, 그래서 디바이스가 손상되면 인간에게 위험하다.

[0039] 본 장치, 시스템, 및 방법의 다양한 예시적인 실시예들은 적절한 솔리드 스테이트 검출기와 짝을 이룬 가스상의 트리튬을 사용함으로써 집적 회로 칩에 통합될 수 있는 매우 컴팩트한 장치를 제작할 수 있음을 보여준다. 소량의 방사성 물질이 배치되기 때문에, 이러한 IC는 설령 디바이스가 파괴되어 방사성 물질이 방출되더라도 사람들을 위험에 빠뜨리는 일 없이 휴대폰들과 같은 소비자 제품들 내부에 사용될 수 있다. IC 칩 상의 TRNG의 제안된 설계에 통합되어야 하는 아날로그 및 디지털 회로들은 솔리드 스테이트 디바이스들을 제작하는 업계 전반에 사용되는 표준 에피택셜(epitaxial), 주입, 및 레이저 어닐링 절차들로 쉽게 제조될 수 있다.

[0040] 본 장치, 시스템, 및 방법의 다양한 예시적인 실시예들은 제조 중에 IC가 방사성 물질로 함침될 수 있음을 보여준다. 예를 들면, 도 1a 내지 도 1d를 참조하자. 매우 소량의 방사성 니켈로도, 각각의 이러한 칩은 초당 수천 개의 랜덤 비트를 생성할 수 있다. 그 다음에 이들 비트는 추후 사용을 위해 IC 내부에 통합된 솔리드 스테이트 메모리에 저장될 수 있다. 그래서, 칩 상의 이러한 독립형 TRNG는 (음성 또는 문자 메시지들과 같은) 통신 채널들의 암호화 또는 (시뮬레이션들 또는 게이밍과 같은) 많은 난수를 필요로 하는 프로세스들에 필요한 수천 개의 멀티 바이트 난수를 수요에 맞춰 쉽게 제공할 수 있다.

[0041] 관련 특허, "트리튬 난수 생성기를 포함하는 장치, 시스템, 및 방법"이라는 발명의 명칭을 갖는 미국 특허 제10,430,161호에는, 온칩 전자 센서에 의해 검출되는 원자핵 붕괴들을 랜덤으로 발생시키는 매체로서 가스상의 트리튬을 사용하는 포괄적인 개념이 기재되어 있다. 이러한 붕괴들의 두 쌍 사이의 시간 지연을 측정 및 비교함으로써, 난수들(비트들)이 생성된다.

[0042] 본 출원에는, 다른 유형의 베타 붕괴가 개시된다. BIPM의 "방사성 핵종 표(Tables of Radionuclides)"를 검색했을 때, 512 keV 미만의 에너지 범위에서 순수한 베타 마이너스 붕괴(전자 방출)를 생성하며 10 년 초과의 타당한 반감기를 갖는 2 개의 핵종만이 발견되었다. M.-M. Be et al. 2008 Bureau International des Poids et Mesures, Sevres (France) BIPM-5 vol. 1 - 4 "Table of Radionucleides"를 참조하라. 감마선은 인클로저들에 사용되는 전형적인 물질들을 투과하므로 고에너지 전자들에 의한 감마선의 생성은 쉽게 차폐될 수 없는 한편 단수명의 동위원소들은 단지 몇 년보다 길게 사용될 수 있는 집적 회로들의 제조에는 적합하지 않기 때문에 제약점들이 관심의 대상이다. 미국 특허 제10,430,161호에서 랜덤성의 근원으로 기재한 트리튬은 약 5.7 keV의 방출된 전자들의 평균 에너지(약 18 keV의 최대 에너지) 및 약 12.3 년(약 4500 일)의 반감기를 갖는 이러한 핵종들 중 하나이다. 그 동위원소의 문제는 매우 투과성이며 그래서 봉쇄가 어려운 그 가스상 형태이다. 발명의 명칭이 "트리튬 기반의 진성 난수 생성기를 위한 방법 및 장치"인 관련 미국 가출원 SN 제62/984,528호에는, 트리튬수(tritiated water)의 사용이 가능케는 방사선 검출기를 덮는 데 사용될 수 있는 겔의 형태로 개시되어 있다.

[0043] 검색에서 발견되었으며 기준을 충족하는 다른 핵종은 원자 번호 63의 니켈 동위원소(기호 ^{63}Ni)이다. 이 동위원소도 저에너지 전자들(평균 에너지 17.4 keV, 최대 에너지 약 67 keV)만을 방출하며 약 98.7 년의 반감기를 갖는다. 이 핵종은 안정된 ^{63}Cu로 붕괴되며, 전형적으로는 원자로 내부에서 중성자들로 ^{62}Ni를 충격을 가함으로써 생성된다. ^{62}Ni의 자연 존재도는 약 3.6 %이다. 그래서, 예를 들면 중성자 조사 전에 원심 분리에 의해 이 동위원소를 농축할 수 있으며, 그에 의해 제조를 비교적 쉽게할 수 있는데, D.F. Williams et al. 1993 Oak Ridge National Laboratory TM-12399 "Recovery and Purification of Nickel-63 from HFIR-irradiated Targets"와 비교해 보라. ^{63}Ni는 의료용 및 다른 베타 검출기들의 교정을 위한 표준으로 사용되므로 상업적으로 이용 가능하다. 이러한 표준들은 니켈을 포함하는 박층들을 다양한 물질들 상에 퇴적함으로써 상이한 방사능으로 제조된다. ^{63}Ni를 염(예를 들면, 염화 니켈)으로 하면 전기도금된 니켈의 두께를 제어(전류 및 시간 프로세스 제어)함으로써 정밀한 양의 방사성 핵종으로 금속 부품들(호일들, 플레이트들)을 덮을 수 있다. 위의 모든 내용은 ^{63}Ni가 집적 회로에 내장된 진성 난수 생성기에 사용되는 방사선 소스에 대한 완벽한 후보임을 시사한다.

[0044] 무게가 63 그램(g)인 ^{63}Ni 1 몰의 자연 방사능은 98.7 년에 걸쳐 아보가드로 수의 절반이거나, 3.1×10^{9} 초 동안

약 3×10^{23} 회의 붕괴 또는 초당 약 10^{14} 회의 붕괴이다. 니켈의 밀도는 약 8.9 g/cm^{3}이므로, 진성 난수 생성기에 실용적이라고 여겨지는 수치인 초당 100 만 회의 붕괴를 얻는 데 필요한 ^{63}Ni의 체적은 0.65 마이크로그램 미만이다. 이들 계산은 방사선이 각 원자핵 주위의 구체(sphere) 전체에서 방출되는 것으로 인해 나중에 적용되는 기하학적 계수는 포함하지 않는다. ^{63}Ni 1 그램의 시장 가격은 $100,000.00 미만이므로, 위에서 언급한 수치 초당 100 만 회의 붕괴에 필요한 ^{63}Ni의 양은 $0.07 미만이다. (그 모든 양의 니켈이 소화되어 신체에 흡수되는 경우에) 사람이 받는 방사선량은 미국 자연 배경 선량의 약 23 %(약 0.7 mSv/년 대 미국 자연 배경의 경우의 3.1 mSv/년)에 상당한다. 이는 본 특허 출원에 따라 이루어진 ^{63}Ni 기반의 TRNG를 실제로 매우 안전하게 한다. 이들 수치는 부록에 제시되어 있다. 이는 각 난수 생성기에 매우 소량의 금속 니켈-63이 필요하며 제조를 비용 효과적이면서 단순화하기 때문에 고무적이다.

[0045] 평균적으로 17.4 keV의 에너지를 갖는 ^{63}Ni의 자발 붕괴에서 방출되는 전자들은 PIN 다이오드(P 및 N 영역은 진성 반도체 영역이 그 사이에 개재된 고농도로 도핑된 반도체들임) 또는 전형적인 CCD 회로로 쉽게 검출될 수 있으며; 이들 디바이스 양자 모두는 TRNG를 갖는 특수 IC의 설계에 쉽게 통합될 수 있다. 도 1a는 공동(22)을 획정하는 인클로저(20) 및 공동(22)을 덮는 캡(15)을 포함하는 이러한 패키징된 IC 설계(5)를 도시한다. 캡(15)은 공동(22)에 노출되는 표면(17)을 갖는다. 도 1b에 나타낸 바와 같이, 캡 표면(17)은 방사성 물질(30)을 포함한다. 검출기/센서(45)는 니켈(30)의 붕괴로부터 유래하는 공동(22) 내의 전자들을 검출하며 검출된 에너지에 대한 신호를 생성한다. 이 검출기/센서(45)는 진성 실리콘 기판 상에 N 형 실리콘과 P 형 실리콘에 의해 형성된 PIN 다이오드일 수 있다. CCD도 검출기로 사용될 수 있다. 비한정적인 예로서 CMOS 전자 센서를 포함하는 다른 유형의 전자 센서들도 사용될 수 있다. 도 1d는 조립된 패키징된 집적 회로(5)를 도시한다.

[0046] 캡(15)은 임의의 금속으로 제작될 수 있고, 일 측면에 원하는 방사능으로 전기도금되며, 제조 프로세스의 마지막에 준비될 수 있다. 이는 상이한 컴포넌트들이 상이한 제조 플랜트에서 조립되고 IC 제조의 최종 단계들에서 신속하게 조립될 수 있게 한다. 매초 약 100 만개의 전자를 방출하는 양의 니켈(30)로 덮인 캡(15)은 이러한 소스로부터 방출되는 전자들이 트리튬에 의해 방출되는 것보다 더 큰 에너지를 가지고 있더라도 인간에게 유해하지 않게 된다. 이러한 소스는 약 0.27 μCi의 활성을 갖는다. 피부의 외측부(10 내지 40 미크론의 두께)에 의해 18 keV 전자들이 완전히 저지된다. M.J. Berger and S.M. Seltzer 1982 National Bureau of Standards NBSIR 82-2550 "Stopping Powers and Ranges of Electrons and Positrons"를 참조하기 바란다. (캡을 삼키는 것과 같이) 체내에 방사성 핵종이 유입되면 약 70 mrem의 선량 - 연간 섭취 한도(Annual Limit for Intake: ALI)는 약 5 rem임 - 에 해당하는 매우 경미한 방사선 위험을 초래한다. Appendix B to 10 CFR Part 20: https://www.nrc.gov/reading-rm/doc-collections/cfr/part020/part020-appb.html를 참조하기 바란다.

[0047] 공기 중(또는 질소와 같은 다른 불활성 가스 중)의 17.4 keV 전자들의 범위는 약 6 mm이며, 그래서 방사성 물질(30)을 갖는 캡(15)은 IC를 갖는 기판(10) 또는 검출기(45)에 접할 필요가 없다. 방사성 물질(30)을 검출기(45)로부터 약 1 mm 미만의 거리만큼 분리하는 것으로 충분하며, 그래도 방출된 전자들의 대부분은 검출기에 부딪히게 된다. 전기도금된 니켈의 두께를 변경함으로써, 초당 붕괴 횟수가 쉽게 제어될 수 있다. 검출기의 면적도 이 수치를 제어할 수 있다. 예를 들면, 0.56 mm^{2}의 면적(예를 들면, 생산에서 더 크게 해야 하는 경우 전자 차단 마스크로 부분적으로 덮일 수 있는 표면을 갖는 750 미크론 × 750 미크론의 PIN 다이오드)과 ^{63}Ni의 약 2 미크론의 활성층을 갖는 검출기는 전자 플럭스가 각 원자핵 주위의 전체 구체(full sphere)로 방출되는 것으로 인해 약 0.07의 기하학적 계수가 고려되면 초당 100 만 카운트 초과를 발생시키게 된다. 전자 발생 물질에서의 전자들의 흡수로 인해, 약 30 ° 의 원뿔형 섹션으로 방출된 전자들의 미소(fraction)만이 방출 구체(emission sphere) 외부의 평평한 표면인 검출기(45)에 도달할 수 있다. 원뿔의 중심으로부터 그 측면까지 측정된 각도 Φ를 갖는 구체의 구형 섹터의 표면의 비율에 대한 공식을 사용하였다.

수학식 1

[0048] $$(1-\cos\Phi)/2$$

[0049] 내장형 검출기를 포함하는 집적 회로의 방사선 손상을 방지하기 위해, 전자들을 방출할 수 있는 ^{63}Ni의 면적은

검출기에 도달하도록 되어 있는 전자들만 열리는 한편 캡 상의 ^{63}Ni 층의 다른 부분들은 100 keV 정도 미만의 에너지를 갖는 전자들을 흡수하는 적어도 100 미크론의 마스킹 물질로 덮일 수 있도록 제한될 수 있다. 캡의 이러한 변형이 도 1c에 제시되어 있다. 캡(15)은 방사성 물질(30)의 층, 및 검출기(45)에 의해 덮이는 영역에 대응하는 윈도 또는 보이드(void)(40)가 있는 마스킹(35)을 갖는다. 마스킹(35)은 페인트를 선택적으로 분사하거나 보이드(40)가 있는 포일 조각을 부착함으로써 쉽게 제조될 수 있다. 캡(15) 상에 퇴적된 방사성 물질(30) 위에 이러한 마스크를 주의하여 배치함으로써, 특히 패시브 영역이 검출기(45) 주위에 남겨지는 경우 집적 회로의 다른 부분들의 방사선 노출이 제한될 수 있다. 이러한 구조에서는 랜덤성의 근원에 의해 방출되는 전자들로부터 집적 회로의 나머지 부분을 효과적으로 차폐하기 위해 약 0.25 ㎜의 정확도면 충분하다.

[0050] 도 2에 나타낸 바와 같이, 검출기(45)는 IC(5)에 포함될 수 있는데, IC(5)는 (저노이즈의 전하에 민감한 전치 증폭기 및 펄스 성형 증폭기와 같은) 증폭기(210), 필터(215), 및 프로세서(220)를 더 포함할 수 있다. 암호화 클라이언트(240)도 선택적으로 IC 상에 있을 수 있다.

[0051] 다음은 위에서 논의된 PIN 다이오드 또는 CCD 유형의 내장 온칩 검출기(45)에 의해 감지되는 전자들의 방출을 초래하는 랜덤 니켈 붕괴를 변환하는 방법이다.

[0052] 1. 니켈 원자핵의 각 붕괴 후에, 약 17.4 KeV의 평균 에너지를 갖는 하나의 전자가 방출된다.

[0053] 2. 각각의 그러한 전자는 바로 그 이벤트의 검출은 가능케 하지만 검출기에 부딪히는 다른 가능한 유형의 고에너지 이온화 입자들의 검출은 가능케 하지 않는 매우 전형적인 시간 프로파일로 검출기(45)에서 전자들의 펄스를 생성한다.

[0054] 3. 검출기(45)로부터의 아날로그 펄스는 증폭기(210)에 의해 증폭된다. 증폭기는 전치 증폭기를 가질 수 있다.

[0055] 4. 증폭기(210)로부터의 증폭된 신호는 디지털 필터(215)에 의해 필터링된다.

[0056] 5. 필터링된 신호는 그 신호가 니켈의 붕괴로 방출된 전자에 대응하며 다른 고에너지 이온화 입자(들)에 의한 것이 아님을 결정하기 위해 프로세서(220)에 의해 처리된다. 프로세서(220)는 이 기능을 수행하는 신호 프로세서(225)를 포함할 수 있다.

[0057] 6. 신호가 실제로 붕괴로 방출된 전자인 경우, 프로세서(220)는 역시 프로세서(220)의 일부일 수 있는 타이머(230)를 시작한다. 시간은 최적으로는 수 GHz의 오더(초당 10^9의 몇 배)의 클럭 주파수일 수 있다. 전자 펄스들은 평균적으로 마이크로초(10^{-6} 초 또는 평균 수천 클럭 틱들(ticks) 사이)마다 검출되기 때문에, 시간적으로 펄스들의 출현의 랜덤성의 차를 검출하기에 충분한 정확도를 갖게 된다.

[0058] 7. 프로세서(220)가 타이머를 중지하도록 트리거하는 후속 붕괴로부터의 제2 펄스를 검출하기 위해 단계 1 내지 6이 반복된다.

[0059] 8. 타이머의 값이 메모리(235)에 저장된다. 이는 도 3a에서 T1로 도시되어 있다.

[0060] 9. 그 다음 2 개의 펄스는 메모리(235)에 저장되는 다른 타이머 값(T2; 도 3a)을 초래한다. T1 및 T2를 생성하기 위해, 도 3a에서는 4 개의 펄스가 사용된다.

[0061] 10. 메모리들에 저장된 2 개의 수치(T1 및 T2)가 비교된다 - 첫 번째 수치가 더 크면 시스템은 값이 1인 비트를 생성하고, 나머지 경우에는 그 값은 0이다. (이 스키마는 물론 반전될 수도 있다.) 이들 비트 값은 메모리(235)에 저장된다. 두 수치가 정확히 같은 매우 드문 상황에서는, 전체 시퀀스가 폐기된다. 그래서, 각 랜덤 비트에 대해, 4 개의 펄스가 사용된다.

[0062] 11. 단계 1 내지 10이 전형적으로는 초당 수십만 회 반복된다.

[0063] 12. 시스템은 전형적으로 256 비트 또는 512 비트 길이의 멀티바이트 수치들을 생성하며, 이들은 칩의 암호화 클라이언트(240)에 의한 추가 사용을 위해 메모리 뱅크에 저장되어, 통신 채널들의 암호화에 필요한 긴(큰) 난수들을 제공한다.

[0064] 13. 수치가 암호 클라이언트(240)에 의해 사용된 후, FILO(first in, last out: 선입후출) 시스템은 다른 수치로 이동하는 한편 전술한 프로세스는 채워질 때까지 메모리에 수치들을 더 추가한다. 이러한 메모리 뱅크가 채워지는 경우에, 메모리에 가장 오래 보관된 수치들은 시스템에 의해 생성되는 새로운 수치들을 위한 공간을 만들기 위해 삭제된다. 이 능력은 시스템이 해킹 등에 대해 훨씬 더 내성을 갖게 한다.

[0065] 시스템은 랜덤 비트당 4 개의 펄스를 사용하지 않을 수도 있다는 점에 유의해야 한다. 대신에, 시스템은 도 3b에 나타낸 바와 같이 구성될 수 있으며, 이 경우 타이머는 각 펄스 검출시에 리셋되며 항상 카운팅하게 된다. 이 시스템의 이점은 랜덤 비트당 3 개의 펄스만을 필요로 한다는 것이다. 그러나, 2 개의 기간은 펄스 이벤트에 의해 연계되기 때문에 서로 다소 종속적이며, 그래서 산출되는 비트 스트링은 도 3a에 제공된 스키마만큼 랜덤하지 않을 수 있으며 랜덤화를 필요로 할 수 있는데, 아래를 참조하기 바란다.

[0066] 난수 생성의 효율을 높이고 간단한 전자 컴포넌트들을 사용하기 위해, 두 쌍의 전자의 검출 사이의 시간들을 측정하고 비교하는 대신에, Patuleanu et al. 2017 Proc. Romanian Acad. series A, vol. 18, 389-402 "True Random Number Sequences From Gamma-Decay Using Four Extraction Methods"를 포함하여, 여러 저자에 의해 2 개의 연속적인 붕괴 사이의 랜덤한 시간들을 측정하면 측정의 최하위 자릿수들(least significant digits)로부터 3 비트가 생성될 수 있다는 것이 시사되었다. 이는 초당 100 만 회의 붕괴로부터 초당 약 1.5 Mbits의 랜덤성이 추출될 수 있음을 의미한다. 생성되는 비트들의 실제 수는 관련된 이벤트들 및 다른 비랜덤 프로세스들을 카운트하는 시스템의 데드 타임으로 인해 야기되는 가능한 바이어스를 제거하는 데 필요한 랜덤화 절차 - J. von Neumann 1951 Res. Nat. Bur. Stand. Appl. Math. Series 3, 36-38 "Various Techniques Used In Connection With Random Digits"와 비교해 보라 - 로 인해 더 적게 된다. 이 정규화의 최신 버전은 2 비트 대신 3 비트를 사용하며, 그래서 프로세스의 효율을 향상시킨다. 예를 들면, B. Skoric 2015 Lecture notes 2IMS10 Technical University Eindhoven (Holland) "Physical Aspects Of Digital Security"를 참조하기 바란다.

[0067] 단일 검출기를 사용하는 대신에, 집적 회로(5)는 전형적인 CCD 광학 매트릭스와 유사한 검출기들의 어레이를 포함할 수 있다. 시스템은 그러한 어레이의 모든 픽셀들의 상태를 판독하고 그 판독으로부터 난수를 생성하기 위해 도 4의 엔트로피 조정 하위단계들/방법(300)을 구현할 수 있다. 예를 들어, 집적 회로(5)는 100 비트의 수를 생성할 수 있는 10×10 어레이를 갖는 검출기(45)를 가질 수 있다. 방금 논의된 타이밍 스키마를 필요로 함이 없이 이 어레이로부터 직접 난수들이 생성될 수 있다. 프로세서는 어레이 내의 각 센서로부터 수신된 신호(전자 타격 여부)를 기초로 1 또는 0을 할당하며, 이들 값은 서로 연결되어 진성 난수들의 어레이를 생성할 수 있다. 이 프로세스는 체커보드에 모래알들을 랜덤하게 떨어뜨리는 것과 같다.

[0068] 그러나 어레이 기반의 TRNG가 실제로 랜덤하며 최적의 엔트로피를 갖는 것을 확실히 하기 위해, 시스템은 엔트로피를 최대로 증가시키기 위해 픽셀들이 50 %의 동일한 확률로 0과 1의 타격을 리포팅하는지를 확인해야 한다. 즉, 10×10 어레이의 모든 1을 더하면 평균적으로 50이 되어야 하고 0도 평균적으로 50이 되어야 한다. 리포팅이 50/50의 최적 역치에 있지 않은 경우, 시스템은 등록 시간을 증가 또는 저감시킬 수 있다(초당 판독 횟수를 저감 또는 증가시킨다: 노출 시간은 역으로 변한다, 즉 판독 횟수를 증가시키면 노출 시간이 감소하고 그 반대도 마찬가지이다). 이 스킴에서는, 동일한 픽셀에의 전자들의 복수의 타격도 여전히 하나의 타격으로 카운트된다.

[0069] 이 자체 조정 방법(300)은 프로세서(220)에서 구현될 수 있는데: 주어진 판독에서의 0의 개수가 사용된 검출기들의 총 개수의 절반보다 작은 경우, 시스템은 판독 시간을 늘려야(초당 판독 횟수는 저감됨) 하며, 반대로 0의 개수가 검출기들의 총 개수의 절반보다 크면 판독 시간을 단축(초당 판독 횟수가 많아짐)시킨다. 이러한 피드백 방법은 신속하게 수렴하게 되며, 그에 따라 여러 판독 사이클의 시간에 걸쳐 평균적으로 일정한 붕괴들의 랜덤률(random rate)로 인해 몇 회의 판독 사이클만 낭비되며, 그래서 매우 정확한 클럭 및 펄스 검출을 필요로 하지 않는 간단한 시스템으로 고품질 비트들을 생성하게 된다.

[0070] 방법(300)은 먼저 판독 속도/노출 시간을 설정하며(305), 다음으로 품질 제어에 사용되는 사이클 수를 설정한다(310). 사이클 내의 판독들로부터, 0이 합계되어 단계 315에서 1의 합계와 비교된다. 이상적으로 이들 개수는 같아야 하지만, 0들의 백분율로 일탈하여 1들보다 크게 시작하면, 시스템은 유사한 백분율로 단계 325에서 판독 속도/노출 시간을 증가시킨다. 그렇지 않으면, 시스템은 단계 330에서 판독 속도/노출 시간을 저감시킨다.

[0071] 메모리는 예를 들면, 이 특수 IC가 장착된 디바이스의 통신 채널들(즉, 암호화 클라이언트(240))의 보안성 랜덤 암호화 또는 시뮬레이션, 모델링, 및 게이밍에 필요한 랜덤 프로세스들에 수요에 맞춰 필요한 바이트(비트) 수를 공급할 수 있다. 생성된 비트들의 랜덤 특성의 실시간 품질 관리가 가능하도록 방법(300)과 같은 난수 시퀀스들의 추가 소프트웨어 테스팅이 IC 칩에 내장될 수 있다. 시퀀스의 일부가 테스트(들)를 통과하지 못하면, 그러한 시퀀스는 제거되어 출력으로 사용되지 않거나, 방법(300)에서와 같이 최적의 엔트로피를 유지하도록 검출기의 판독 속도가 조정될 수 있다. 이러한 유형의 교정은 칩에 의해 생성되는 시퀀스들의 랜덤 특성을 더욱 향상시킨다.

[0072] 본 장치, 시스템, 및 방법의 다양한 예시적인 실시예들은 표준 반도체 생산 라인에서 TRNG IC들을 제조하는 능력을 제공하는데, 유일한 차이점은 패키징이 약 0.5 mm^2 크기의 검출기 및 유사한 형상을 갖는 마스크로 차폐되고 검출기 위에 배치된 전기도금 니켈-63이 있는 엔클로저의 캡을 위에서 계산된 바와 같이 남겨두어야 한다는 것이다. 그렇지 않으면, 니켈의 붕괴 중에 방출되는 전자들이 IC의 보호 물질을 관통할 수 없기 때문에 생산된 IC들은 소비재의 제조에 전형적으로 사용되는 다른 IC들과 설계 및 다른 특성 면에서 매우 유사하게 된다. 플라스틱과 같은 물질에서의 18 keV 전자들의 범위는 3 마이크로미터 미만이다. 패키징은 동등하거나 훨씬 더 높은 에너지의 임의의 외부 방사선으로부터 내장형 검출기를 차폐하게 된다. 이러한 고에너지 입자들이 패키징 인클로저를 통과하게 되더라도, 이들은 다른 유형의 펄스들을 생성하게 되며, 이들은 난수들을 생성하는 데 사용되는 18 keV의 펄스들로부터 필터링함으로써 구별될 수 있다.

[0073] 본 기술분야의 통상의 기술자에게 명백하다시피 본 명세서에 기재되고 통합된 적절한 기술들, 재료들, 및 설계들 중 임의의 것이 본 발명의 다양한 예시적인 양태들을 구현하는 데 사용될 수 있다.

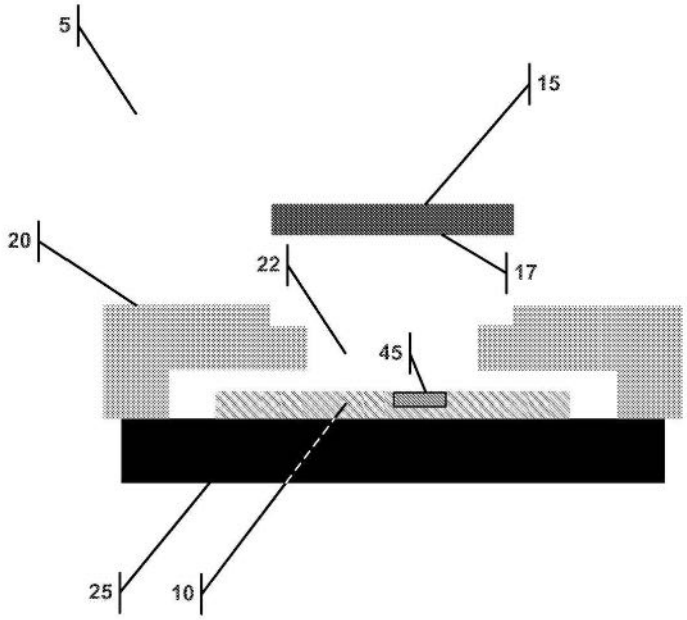
[0074] 본 발명의 예시적인 실시예들과 적용들이 위에서 설명되고 포함된 예시적인 도면들에 도시된 것을 포함하여 본 명세서에 설명되었으나, 본 발명이 이들 예시적인 실시예와 적용에 국한되거나 예시적인 실시예들과 적용들이 동작하거나 본 명세서에 기재된 방식에 국한되는 것을 의도하지는 않는다. 실제로, 본 기술분야의 통상의 기술자에게 분명하다시피 예시적인 실시예들에 대한 많은 변경 및 변형이 가능하다. 산출되는 디바이스, 시스템, 또는 방법이 본 특허 출원 또는 임의의 관련된 특허 출원을 기초로 특허청이 허여하는 청구범위 중 하나의 범위 내에 있는 한 본 발명은 임의의 디바이스, 구조, 방법, 또는 기능을 포함할 수 있다.

[0075] **부록**

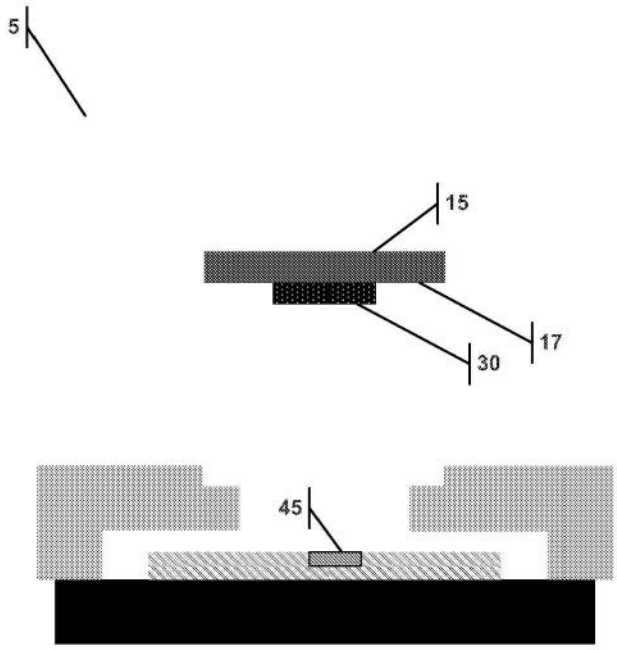
[0076]	^{63}Ni의 밀도	63 g/mol
[0077]	반감기	98.7 년
[0078]		3,112,603,200 초
[0079]	TRNG 필요치	1,000,000 붕괴/초
[0080]		1 붕괴/마이크로초
[0081]	방사능	1,000,000 Bq
[0082]		$2.70*10^{-5}$ Ci(붕괴당 17.4 keV의 e^- 에너지)
[0083]	신체당 선량	80 kg 신체에 대해 $2.23*10^{-10}$ J/(kg · s)
[0084]		$7.02*10^{-3}$ Gy/년
[0085]		0.70 mSv/년; 미국 자연 배경 E_{US}=3.1 mSv/년
[0086]		미국 연간 자연 배경 선량의 23 %
[0087]		(니켈 전량이 체내에 흡수된 경우)
[0088]	10^6 붕괴/초를 위한 ^{63}Ni	$6.51*10^{-7}$ g
[0089]	필요한 ^{63}Ni의 비용	$0.07($^{63}Ni 비용은 $100,000/그램 미만)
[0090]	검출기 크기	0.56 mm^2 0.75 mm × 0.75 mm
[0091]	활성층 두께	2.0 μm
[0092]	활성 ^{63}Ni의 체적	0.0011 mm^3
[0093]	필요한 ^{63}Ni의 질량	10.0 μg
[0094]	카운트	$1.03*10^6$ 카운트/초(기하학적 계수 0.07 포함)

도면

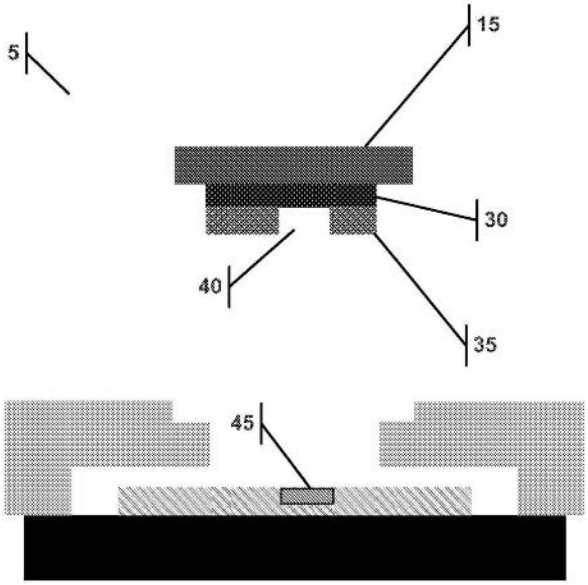
도면1a



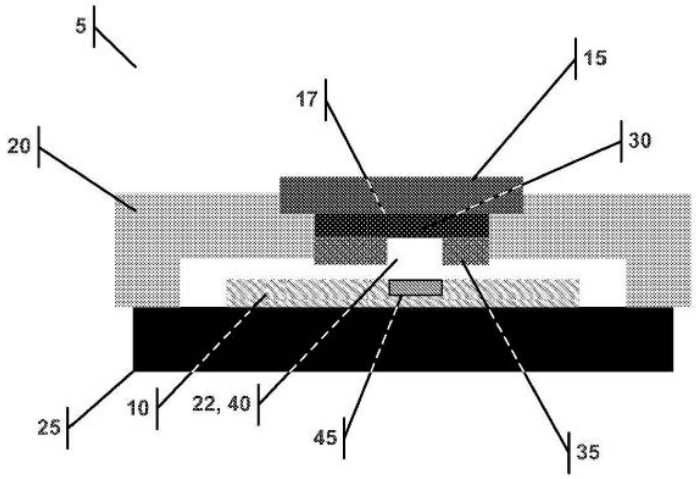
도면1b



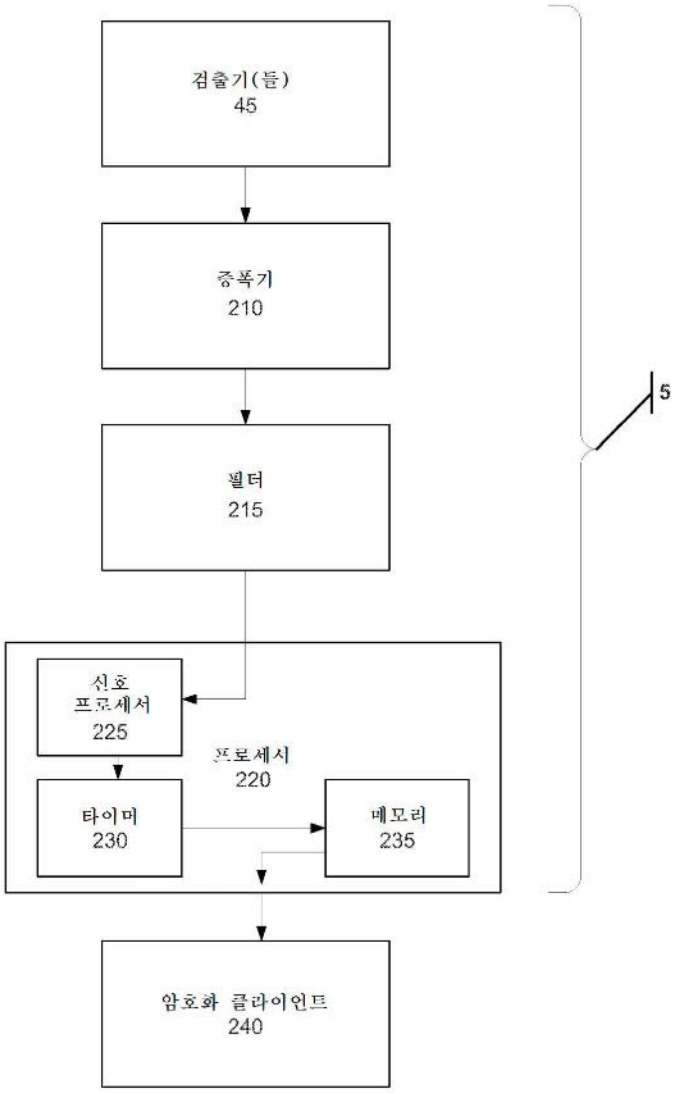
도면1c



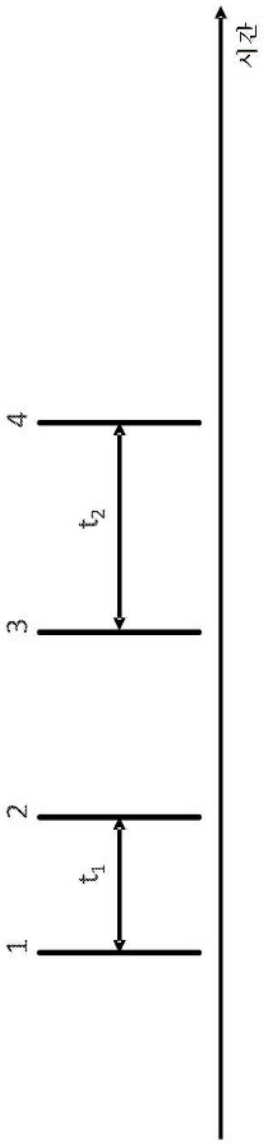
도면1d



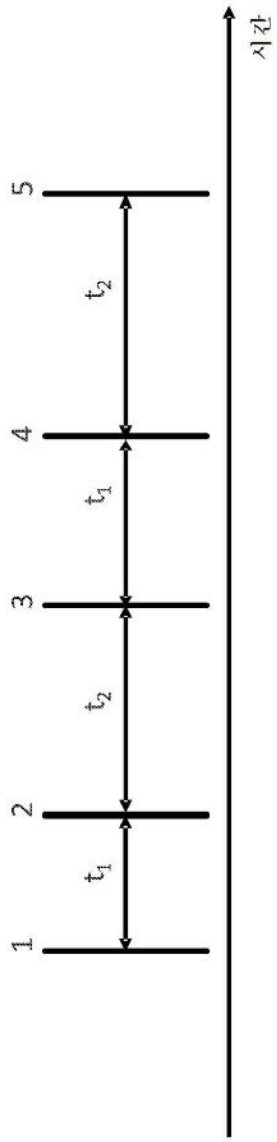
도면2


검출기(들)
45
증폭기
210
필터
215
신호
프로세서
225
프로세싱
220
타이머
230
메모리
235
암호화 클라이언트
240
5

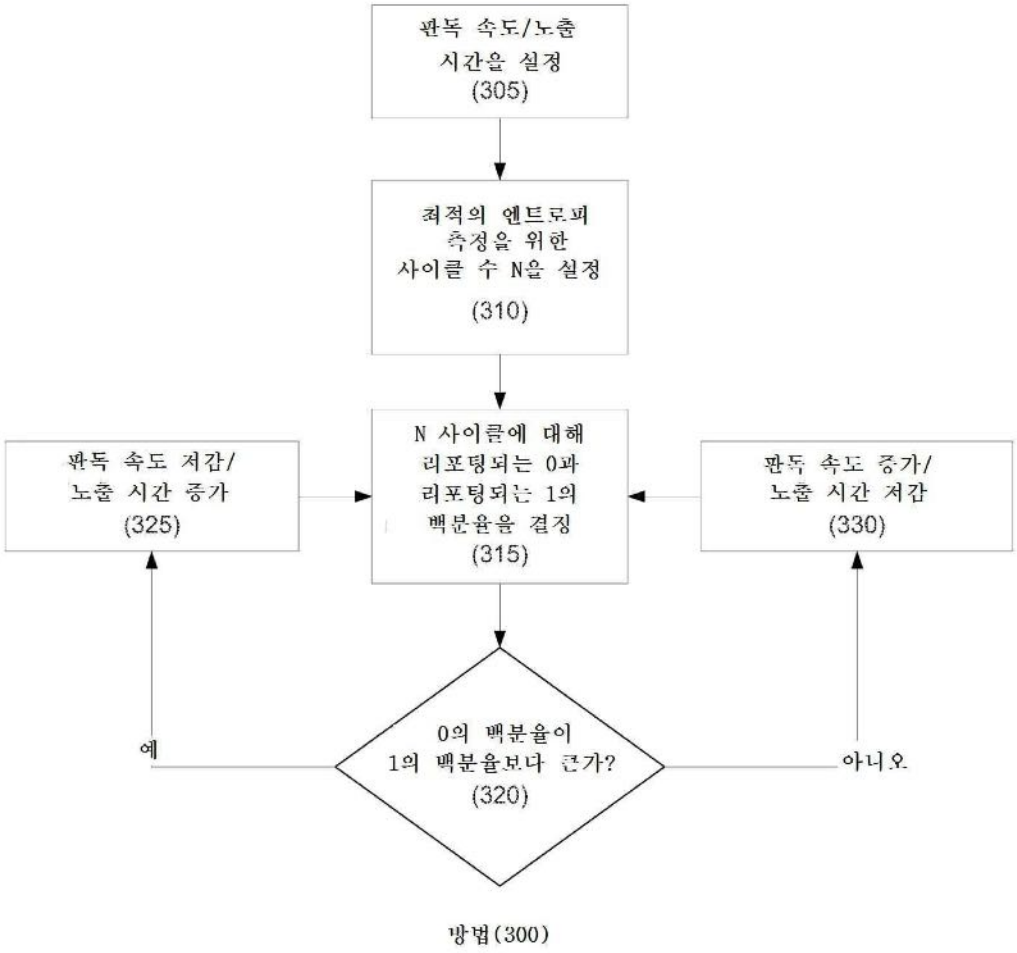
도면3a



도면3b



도면4



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 7

【변경전】

제6 항에 있어서,

상기 프로세서는 상기 진성 난수들의 어레이를 암호화 클라이언트에 제공하며; 전달된 진성 난수를 상기 메모리에서 삭제하는,

TRNG.

【변경후】

제6 항에 있어서,

상기 프로세서는 상기 진성 난수들의 어레이를 암호화 클라이언트에 제공하며; 전달된 진성 난수를 메모리에서 삭제하는,

TRNG.

【직권보정 2】

【보정항목】 청구범위

【보정세부항목】 청구항 9

【변경전】

제6 항에 있어서,

상기 메모리가 가득 차면, 상기 프로세서는 상기 진성 난수들의 어레이에서 가장 오래된 것을 삭제하는,

TRNG.

【변경후】

제6 항에 있어서,

메모리가 가득 차면, 상기 프로세서는 상기 진성 난수들의 어레이에서 가장 오래된 것을 삭제하는,

TRNG.

【직권보정 3】

【보정항목】 청구범위

【보정세부항목】 청구항 17

【변경전】

진성 난수 생성기로서, 집적 회로의 표면 위에 공동을 획정하는 인클로저; 상기 공동에 노출된 캡 표면 - 상기 캡 표면은 방사성 니켈을 포함함 - 으로 상기 공동을 덮는 캡; 상기 방사성 니켈의 일부의 위에 적용되며 상기 방사성 니켈에 의해 상기 공동 내로 방출되는 전자들의 양과 방향을 제한하도록 구성된 마스크를 포함하고; 상기 IC는: 상기 캡 표면으로부터 상기 공동의 건너편에 소정 거리에 위치된 전자 센서 - 상기 전자 센서는 상기 공동 내의 상기 방사성 니켈에 의해 방출되는 전자들을 검출하고 상기 검출된 전자들에 대한 신호를 발생시키도록 상기 마스크의 보이드와 정렬되도록 구성됨 -; 상기 전자 센서에 연결되고 상기 신호를 증폭하도록 구성된 증폭기; 상기 신호를 필터링하도록 구성된 상기 증폭기에 연결된 필터; 상기 필터에 연결된 프로세서 - 상기 프로세서는 상기 신호를 기초로 진성 난수를 생성하도록 구성됨 - 를 포함하며; 상기 마스크는 상기 방사성 니켈에 의해 방출되는 전자들로부터 상기 증폭기, 필터, 및 프로세서를 적어도 부분적으로 차폐하는, 상기 진성 난수 생성기; 및

상기 진성 난수를 수신하도록 적합화된 암호화 클라이언트:

를 포함하는, 개인용 전자 디바이스.

【변경후】

진성 난수 생성기로서, 집적 회로(integrated circuit: IC)의 표면 위에 공동을 획정하는 인클로저; 상기 공동에 노출된 캡 표면 - 상기 캡 표면은 방사성 니켈을 포함함 - 으로 상기 공동을 덮는 캡; 상기 방사성 니켈의 일부의 위에 적용되며 상기 방사성 니켈에 의해 상기 공동 내로 방출되는 전자들의 양과 방향을 제한하도록 구성된 마스크를 포함하고; 상기 IC는: 상기 캡 표면으로부터 상기 공동의 건너편에 소정 거리에 위치된 전자 센서 - 상기 전자 센서는 상기 공동 내의 상기 방사성 니켈에 의해 방출되는 전자들을 검출하고 상기 검출된 전자들에 대한 신호를 발생시키도록 상기 마스크의 보이드와 정렬되도록 구성됨 -; 상기 전자 센서에 연결되고 상기 신호를 증폭하도록 구성된 증폭기; 상기 신호를 필터링하도록 구성된 상기 증폭기에 연결된 필터; 상기 필터에 연결된 프로세서 - 상기 프로세서는 상기 신호를 기초로 진성 난수를 생성하도록 구성됨 - 를 포함하며; 상기 마스크는 상기 방사성 니켈에 의해 방출되는 전자들로부터 상기 증폭기, 필터, 및 프로세서를 적어도 부분적으로 차폐하는, 상기 진성 난수 생성기; 및

상기 진성 난수를 수신하도록 적합화된 암호화 클라이언트:

를 포함하는, 개인용 전자 디바이스.