(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2022년08월03일
(11) 등록번호 10-2429142
(24) 등록일자 2022년08월01일

(51) 국제특허분류(Int. Cl.)
G06F 7/58 (2006.01) *G21H 5/00* (2015.01)
(52) CPC특허분류
G06F 7/588 (2013.01)
G21H 5/00 (2018.05)
(21) 출원번호 10-2022-0018892
(22) 출원일자 2022년02월14일
심사청구일자 2022년03월08일
(30) 우선권주장
63/224,811 2021년07월22일 미국(US)
(56) 선행기술조사문헌
KR1020190057065 A
KR1020200119459 A

(73) 특허권자
란데몬 에스피. 제트 오.오.
폴란드 바르샤바 02-858 유엘. 크사웨로우 21
(72) 발명자
쿠지미츠, 비스와프 보그단
미국 캘리포니아 92011 칼즈배드 스위트 104-381 아베니다 엔시니타스 7040
타타르키비츠, 잔 제이컵
미국 캘리포니아 92011 칼즈배드 스위트 104-381 아베니다 엔시니타스 7040
(74) 대리인
김정훈

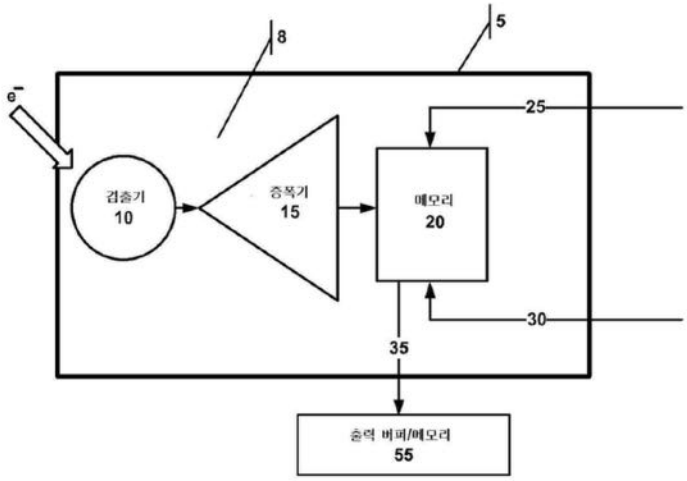
전체 청구항 수 : 총 17 항 심사관 : 지정훈

(54) 발명의 명칭 **베타 붕괴를 이용한 고도로 효과적인 온칩 진성 난수 생성기를 위한 방법 및 장치**

(57) 요 약

방사선 소스(바람직하게는 방사성 니켈), 및 셀들의 선형 어레이로부터 방사성 니켈을 분리하는 공동을 둘러싸는 인클로저를 포함하는, 진성 난수 생성기(TRNG)가 개시된다. 셀들은 니켈의 붕괴로부터 공동 내의 전자들을 검출하고 검출된 에너지에 대한 신호를 생성하도록 구성된 검출기를 갖는 실리콘 기판을 포함한다. 검출기에 연결된 증폭기는 신호를 증폭하여 저장을 위해 메모리로 전달한다. 제어 블록이 선형 어레이의 각 셀에 연결되고, (a) 각 셀에 워드 라인 신호를 송신하여, 메모리가 비트 라인을 통해 출력 버퍼/메모리에 그 콘텐츠를 리포트하게 하며, 또한 (b) 각 셀에 리셋 신호를 송신하여, 메모리를 삭제하게 한다.

대 표 도



명 세 서

청구범위

청구항 1

방사성 니켈;

상기 방사성 니켈을 셀들의 선형 어레이 - 상기 선형 어레이 내의 각 셀은:

상기 니켈의 붕괴로부터 공동(cavity) 내의 전자들을 검출하고 상기 검출된 에너지에 대한 신호를 생성하도록 구성된 검출기;

상기 검출기에 연결되고 상기 신호를 증폭하도록 구성된 증폭기; 및

상기 증폭기에 연결되고 상기 신호를 저장하도록 구성된 메모리:

를 포함하는 실리콘 기판:

을 포함함 - 로부터 분리하는 공동; 및

상기 선형 어레이 내의 각 셀에 연결되고, (a) 각 셀에 워드 라인 신호(word line signal)를 송신하여 상기 메모리가 비트 라인(bit line)을 통해 출력 버퍼/메모리에 그 콘텐츠를 리포트하게 하며; 및 (b) 각 셀에 리셋 신호를 송신하여 메모리를 삭제하게 하도록 구성된 제어 블록:

을 둘러싸는 인클로저:

를 포함하는, 진성 난수 생성기(true random number generator: TRNG).

청구항 2

제1 항에 있어서,

처리 회로는 관통 실리콘 비아(through silicon via: TSV)로 상기 검출기에 연결되고, 상기 실리콘 기판은 상기 방사성 니켈에 의해 방출되는 전자들로부터 상기 처리 회로를 적어도 부분적으로 차폐하며, 상기 처리 회로는 다음의: 상기 증폭기, 상기 메모리, 및 상기 제어 블록 중 하나 이상을 포함하는,

TRNG.

청구항 3

제1 항에 있어서,

상기 TRNG는 상기 제어 블록에 연결된 클럭을 더 포함하고, 상기 제어 블록은 상기 셀들의 선형 어레이에 대한 상기 워드 라인 신호 및 상기 리셋 신호를 관리하기 위해 상기 클럭을 사용하는,

TRNG.

청구항 4

제3 항에 있어서,

각 셀의 상기 출력 버퍼/메모리에 연결된 시리얼 인터페이스를 더 포함하는, TRNG.

청구항 5

제4 항에 있어서,

상기 시리얼 인터페이스는 복수의 시리얼 인터페이스를 포함하는,

TRNG.

청구항 6

제5 항에 있어서,

상기 클럭은 저속 클럭과 고속 클럭을 포함하며, 상기 제어 블록은 상기 워드 라인 신호를 관리하기 위해 상기 고속 클럭을 사용하고 상기 리셋 신호를 관리하기 위해 상기 저속 클럭을 사용하는,

TRNG.

청구항 7

제6 항에 있어서,

상기 클럭은 상기 저속 클럭과 상기 고속 클럭 사이의 관계를 유지하기 위한 주파수 분주기를 더 포함하는,

TRNG.

청구항 8

제1 항에 있어서,

상기 선형 어레이 내의 각 셀은 상기 증폭기에 연결된 전송 게이트를 포함하는,

TRNG.

청구항 9

제8 항에 있어서,

리셋 신호들 사이의 시간은 독출 기간(readout period)을 규정하고, 상기 TRNG는 각 셀의 상기 전송 게이트에 연결된 OR 게이트를 더 포함하며, 각 셀에 대해, 상기 OR 게이트는 상기 검출기가 상기 니켈의 붕괴로부터 상기 공동 내의 전자들을 검출할 때 독출 기간 동안 카운터에 단일의 카운팅 신호를 생성하도록 적합화되는,

TRNG.

청구항 10

제9 항에 있어서,

상기 카운터는 카운팅 신호들의 사전 결정된 개수가 카운팅되었을 때 상기 제어 블록에 정지 신호를 송신하도록 구성되는,

TRNG.

청구항 11

제9 항에 있어서,

상기 카운터는 카운팅 신호들의 사전 결정된 개수가 카운팅되었을 때 자체적으로 리셋하도록 구성되는,

TRNG.

청구항 12

제10 항에 있어서,

상기 정지 신호에 응답하여, 상기 제어 블록은 상기 워드 라인 신호와 상기 리셋 신호를 각 셀에 송신하는,

TRNG.

청구항 13

제9 항에 있어서,

상기 카운팅 신호들의 사전 결정된 개수는 512인,

TRNG.

청구항 14

제1 항에 있어서,

암호화 클라이언트를 더 포함하는, TRNG.

청구항 15

제1 항에 있어서,

상기 선형 어레이는 1024개의 셀을 포함하는,

TRNG.

청구항 16

제1 항에 있어서,

상기 셀들의 선형 어레이의 매트릭스를 더 포함하는, TRNG.

청구항 17

제16 항에 있어서,

상기 매트릭스는 1024 x 1024의 셀로 구성되는,

TRNG.

발명의 설명

기 술 분 야

[0001] 본 발명은 일반적으로 진성 난수 생성기들, 구체적으로는 자발적 니켈 동위원소 붕괴를 이용한 난수 생성기 기술들, 및 이에 관한 장치들, 시스템들, 및 방법들에 관한 것이다.

배 경 기 술

[0002] 우선권 출원들 및 참고 문헌들

[0003] 본 출원은 발명의 명칭이 "베타 붕괴를 이용한 고도로 효과적인 온칩 진성 난수 생성기를 위한 방법 및 장치"이며 2021년 8월 24일자로 제출되고, 현재는 XXXXX자로 허여된 미국 특허 XXXXX호인 미국 출원 제17/409971호; 발명의 명칭이 "고도로 효과적인 베타 붕괴 기반의 온칩 진성 난수 생성기를 위한 방법 및 장치"이며 2021년 7월 22일자로 제출된 미국 가출원 SN 제63/224811호; 발명의 명칭이 "고도로 효과적인 베타 붕괴 기반의 온칩 진성 난수 생성기를 위한 방법 및 장치"이며 2021년 8월 19일자로 제출된 미국 가출원 SN 제63/234820호; 및 발명의 명칭이 "고도로 효과적인 베타 붕괴 기반의 온칩 진성 난수 생성기를 위한 방법 및 장치"이며 2021년 8월 19일자로 제출된 미국 가출원 SN 제63/235031호의 우선권을 주장하는데, 이들 모두는 그 전체가 참조로 본 명세서에 편입되어 있다.

[0004] 본 출원은 2020년 3월 3일자로 제출되고 발명의 명칭이 "트리튬 기반의 진성 난수 생성기를 위한 방법 및 장치"인 미국 가출원 SN 제62/984,528호; 2020년 8월 7일자로 제출되고 발명의 명칭이 "베타 붕괴 기반의 진성 난수 생성기를 위한 방법 및 장치"인 미국 가출원 SN 제63/062,672호; 2018년 4월 9일자로 제출되고 발명의 명칭이 "트리튬 난수 생성기를 포함하는 장치, 시스템, 및 방법"인 미국 가출원 SN 제62/655,172호; 2019년 2월 9일자로 제출되고 발명의 명칭이 "트리튬 난수 생성기를 포함하는 장치, 시스템, 및 방법"이며 현재는 미국 특허 제10,430,161호인 미국 가출원 SN 제62/803,476호; 2019년 2월 12일자로 제출되고 발명의 명칭이 "트리튬 난수 생성기를 포함하는 장치, 시스템, 및 방법"인 미국 출원 SN 제16/273,365호; 2020년 8월 11일자로 제출되고 발명의 명칭이 '베타 붕괴 기반의 진성 난수 생성기를 위한 장치, 시스템, 및 방법'이며 현재는 미국 특허 제10,901,695호인 미국 출원 제16/990,087호; 2020년 12월 18일자로 제출되고 발명의 명칭이 "트리튬 기반의 진성 난수 생성기를 위한 방법 및 장치"이며 현재는 미국 특허 제11,048,478호인 미국 출원 제17/126,265호; 2020년 10월 2일자로 제출되고 발명의 명칭이 "베타 붕괴 기반의 진성 난수 생성기를 위한 장치, 시스템, 및 방법"이며 현재는 미국 특허 제11,036,473호인 미국 출원 제17/062,307호; 발명의 명칭이 "트리튬 난수 생성기를 포함하는

장치, 시스템 및 방법"이며 2019년 2월 13일자로 제출된 PCT 출원 PCT/US19/17748; 발명의 명칭이 "베타 붕괴 기반의 진성 난수 생성기를 위한 장치, 시스템, 및 방법"이며 2020년 12월 18일자로 제출된 PCT 출원 PCT/US20/65962; 및 발명의 명칭이 "베타 붕괴 기반의 진성 난수 생성기를 위한 장치, 시스템, 및 방법"이며 2020년 12월 18일자로 제출된 PCT 출원 PCT/US20/65976에도 또한 관련된다. 본 명세서에서 논의 및/또는 인용된 특허 출원들, 허여된 특허들, 및 기타 참고 문헌들 각각은 마치 본 명세서에 전체가 기재된 것처럼 참조로 편입되어 있다.

[0005] 본 명세서에서 참조되고 또한 편입되어 있는 것들은 다음과 같다: (1) M.-M. Be et al., 2008 Bureau International des Poids et Mesures, Sevres (France) BIPM-5 vol. 1 - 7, "Table of Radionuclides"; (2) Belghachi A. et al., 2020 Acta Physica Polonica A vol. 137, no. 3, pp. 324 - 331, *A model of Ni-63 source for betavoltaic application*; 및 (3) Knechtel J. et al., 2017 PSJ Transactions on System LSI Design Methodology vol. 10 pp. 45-62 *Large-Scale 3D Chips: Challenges and Solutions for Design Automation, Testing, and Trustworthy Integration*.

발명의 내용

[0006] 수치 알고리즘들에 기초한 의사(pseudo) 난수 생성기들과 대조적으로, 자연적인 랜덤 프로세스들: 복수의 바이폴라 스위치, 열 잡음, 다이크로익 미러들(dichroic mirrors)에 의한 광 산란, 카오스 시스템들, 및 방사성 핵들의 붕괴에 의존하는 진성 난수 생성기(true random number generator: TRNG) 디바이스들이 있다. 이들 TRNG 중 몇 가지는 본 출원이 우선권을 주장하는 가출원들에 열거되어 있으며, 이들 참고 문헌들은 마치 본 명세서에 전체가 기재된 것처럼 참조로 본 명세서에 편입되어 있다.

[0007] 방사성 핵종의 붕괴는 온도, 압력, 또는 가속도와 같은 환경적 영향들로부터 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 핵은 고도로 방사성 및 유독성이며, 그래서 디바이스가 손상되면 인간에게 위험하다.

[0008] 따라서, 사용자를 위험한 수준의 방사선에 노출시키지 않는 안전하고 소형인 TRNG가 유리하다 할 것이다. 이러한 TRNG는 그래서 컴팩트한 개인용 디바이스들에 사용될 수 있다.

[0009] 방사선 소스(바람직하게는 방사성 니켈) 및 방사성 니켈을 셀들의 선형 어레이로부터 분리하는 공동(cavity)을 둘러싸는 인클로저를 갖는 진성 난수 생성기(true random number generator: TRNG)가 개시된다. 셀들은 니켈의 붕괴로부터 공동 내의 방출된 전자들을 검출하고 검출된 에너지에 대한 신호를 생성하도록 구성된 검출기를 갖는 실리콘 기판을 포함한다. 검출기에 연결된 증폭기는 신호를 증폭하고 저장을 위해 이를 메모리로 전달한다. 선형 어레이 내의 각 셀에 연결된 제어 블록은 (a) 각 셀에 워드 라인 신호(word line signal)를 송신하여, 메모리가 비트 라인(bit line)을 통해 출력 버퍼/메모리에 그 콘텐츠를 리포트하게 하며, 또한 (b) 각 셀에 리셋 신호를 송신하여, 메모리를 삭제하게 한다.

[0010] 처리 회로는 실리콘 기판이 방사성 니켈에 의해 방출되는 전자들로부터 처리 회로를 적어도 부분적으로 차폐하도록 관통 실리콘 비아(through silicon via: TSV)로 검출기에 연결될 수 있다. 처리 회로는 다음의: 증폭기, 메모리, 및 제어 블록 중 하나 이상을 포함한다.

[0011] 클럭이 제어 블록에 연결될 수 있고, 제어 블록은 다시 셀들의 선형 어레이에 대한 워드 라인 신호 및 리셋 신호를 관리하기 위해 클럭을 사용한다. 시리얼 인터페이스 또는 복수의 시리얼 인터페이스가 각 셀의 출력 버퍼/메모리에 연결될 수 있다.

[0012] 클럭은 저속 클럭과 고속 클럭을 포함할 수 있다. 제어 블록은 워드 라인 신호를 관리하기 위해 고속 클럭을 사용할 수 있고 리셋 신호를 관리하기 위해 저속 클럭을 사용할 수 있다. 클럭은 저속 클럭과 고속 클럭 사이의 관계를 유지하기 위한 주파수 분주기를 또한 가질 수 있다.

[0013] 리셋 신호들 사이의 시간은 독출 기간(readout period)을 규정하고, TRNG는 각 셀의 전송 게이트에 연결된 OR 게이트를 더 포함할 수 있다. 각 셀에 대해, OR 게이트는 독출 기간 동안에 하지만 검출기가 니켈의 붕괴로부터 공동 내의 전자들을 검출할 때에만 카운터에 단일의 카운팅 신호를 생성한다. 카운터는 카운팅 신호들의 사전 결정된 개수가 카운팅되었을 때 제어 블록에 정지 신호를 송신하고, 또한 자체적으로 리셋한다. 정지 신호의 수신 시에, 제어 블록은 워드 라인 신호와 리셋 신호를 각 셀에 송신한다. 카운팅 신호들의 사전 결정된 개수는 512일 수 있으나, 이에 국한되지는 않는다.

[0014] TRNG는 암호화 클라이언트를 더 포함할 수 있고, 선형 어레이들의 매트릭스로 구성될 수 있다. 선형 어레이는 1024개의 셀로 구성될 수 있으나 이에 국한되지는 않는다. TRNG는 1024 x 1024 셀의 매트릭스를 가질 수 있으나 이에 국한되지는 않는다.

[0015] 본 기술분야의 통상의 기술자에게 분명한 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 달리 확립하지 않는다.

도면의 간단한 설명

[0016] 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 1은 검출기의 전자 충돌(electron hits)을 등록하는 회로를 도시한다.

도 2는 n개의 셀 - 각각 아래에 그 처리 셀을 가짐 - 의 선형 어레이의 배치를 나타낸다.

도 3은 선형 어레이들의 매트릭스를 도시한다.

도 4는 선형 어레이들의 매트릭스 내에 사용되는 시리얼 인터페이스 회로를 도시한다.

도 5는 "관찰된 검출들" 또는 적어도 하나의 전자 충돌을 등록한 검출기들의 개수를 도시하는 그래프인 한편, "필요한 붕괴들"은 "관찰된 검출" 값들을 얻기 위해 생성되어야 하는 전자들의 개수이다.

도 6은 OR 게이트가 사용된, 검출기의 전자 충돌을 등록하기 위한 대체 회로를 도시한다.

도 7은 n개의 검출기 - 각각 아래에 그 처리 셀을 가짐 - 의 선형 어레이의 배치를 나타낸다.

도 8a는 검출기들의 어레이가 보일 수 있도록 커버와 방사성 소스가 반투명하게 된 셀 어레이 매트릭스를 갖는 검출기 칩의 평면도이다.

도 8b는 셀 어레이 매트릭스 내의 단일 검출기 칩의 일부의 단면도로서, 도 8a의 셀 어레이는 관통 실리콘 비아를 사용하여 검출기의 전자 충돌을 등록하기 위한 회로를 도시한다.

도 9는 도 4의 배치에 대응하는 집적 회로 상에 배치될 수 있는 다양한 컴포넌트들의 흐름도이다.

도 10은 도 7의 배치에 대응하는 집적 회로 상에 배치될 수 있는 다양한 컴포넌트들의 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0017] 본 명세서에서는 본 발명을 수행하기 위해 본 발명자에 의해 구상되는 임의의 최상의 모드들을 포함하여, 본 발명의 몇몇 구체적인 예에 대해 참조가 이루어진다. 이들 구체적인 실시예의 예들은 첨부 도면들에 도시되어 있다. 본 발명이 이들 구체적인 실시예와 연계하여 설명되지만, 본 발명을 설명되거나 도시된 실시예들로 한정하고자 함이 아님을 이해할 것이다. 오히려, 첨부된 청구범위에 의해 규정되는 본 발명의 사상과 범위 내에 포함될 수 있는 대체물들, 변형들, 및 등가물들을 포함하도록 의도된다.

[0018] 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 특정 실시예들에서는 반드시 나타낸 순서로 수행되는 것은 아니며, 또는 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 2개 이상의 엔티티 사이의 연결, 관계, 또는 통신을 기

술하게 된다. 임의의 2개의 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.

[0019] 다음의 예시적인 특징부들의 목록은 첨부 도면들에 대응하며 참조의 편의를 위해 제공되는데, 동일한 참조 번호들은 명세서와 도면들 전체에 걸쳐 대응하는 특징부들을 가리킨다.

[0020] 5: 셀

[0021] 5A: 셀

[0022] 8: 실리콘 기판

[0023] 10: 검출기

[0024] 15: 증폭기

[0025] 20: 메모리

[0026] 25: 워드 라인

[0027] 30: 리셋 라인

[0028] 35: 비트 라인(bit line)

[0029] 40: 셀 선형 어레이

[0030] 40A: 셀 선형 어레이

[0031] 45: 제어 블록

[0032] 50: 클럭

[0033] 50A: 저속 클럭

[0034] 50B: 고속 클럭

[0035] 50C: 주파수 분주기

[0036] 55: 출력 버퍼/메모리

[0037] 60: 출력 비트

[0038] 65: M x P 셀 어레이 매트릭스

[0039] 70: 시리얼 인터페이스

[0040] 72: 전송 게이트

[0041] 74: 전송 게이트 제어 신호

[0042] 75: OR 게이트

[0043] 80: 카운터

[0044] 82: 정지 신호

[0045] 85: 셀 어레이 매트릭스를 갖는 TRNG 검출기 칩

[0046] 90: 칩 커버/인클로저

[0047] 95: 방사성 소스

[0048] 100: 공동

[0049] 105: 관통 실리콘 비아/연결부

[0050] 110: 처리 회로

[0051] 115: 암호화 클라이언트

[0052] 본 설명은 위에 열거된 이전에 공개된 미국 특허들 및 출원들에 관련되는데, 이들 문헌에서는 전자 센서 또는 센서들의 어레이를 통해 온칩(on-chip)에서 방출된 전자들을 검출함으로써 순수한 베타 마이너스(전자 방출) 핵 붕괴를 진성 난수들을 생성하기 위한 매체 또는 엔트로피 소스로 사용하는 개괄적인 개념을 설명하였다. 이 출원에서는, 동일한 엔트로피 소스, 즉 ^{63}Ni로부터 온칩에서 훨씬 더 빠르고 더 효율적인(시간 단위당 더 큰 비트 수) 난수 생성을 가능케 하는 접근법을 제시하고자 한다.

[0053] BIPM의 "방사성 핵종 표(Tables of Radionuclides)(2008)"를 검색하면, (고도로 투과성의 감마선을 발생시켜, 잠재적인 방사선 위험을 초래하는 전자들의 에너지를 회피하기 위해) 512 keV 미만의 에너지의 범위에서 (전자의 방출만 및 일부 실제로 검출할 수 없는 중성미자의 운동량을 보존하기 위해) 순수한 베타 마이너스 붕괴를 발생시키며 10년 초과의 타당한 반감기를 갖는 3개의 풍부한 핵종을 발견한다. 우리의 요건을 충족하는 위에서 언급된 표들에 열거된 몇몇 다른 외래 핵종이 있으나, 이들은 대부분 다른 외래 핵종들의 붕괴의 부산물들이며, 그래서 산업 용도로는 실용적이지 않는다. 획득 및 처리가 가장 용이한 3가지 핵종은 다음과 같다:

[0054] a. 1. 방출되는 전자들의 최대 에너지가 18 keV(평균 에너지는 약 5.7 keV)이고 반감기가 약 12.4년인 ^{3}H 트리튬,

[0055] b. 2. 방출되는 전자들의 최대 에너지가 약 67 keV(평균 에너지는 약 17 keV)이고 반감기가 약 98.7년인 ^{63}Ni 니켈, 및

[0056] c. 3. 방출되는 전자들의 최대 에너지가 약 156 keV(평균 에너지는 약 45 keV)이고 반감기가 약 5,700년인 ^{14}C 탄소.

[0057] (미국 특허 제11,048,478호에서 논의된 바와 같이, 고체들을 통한 그 높은 투과성으로 인해 취급이 매우 어려우며, 그래서 젤이나 고체 화합물의 형태로 보다 양호하게 처리되는 가스상 트리튬의 경우를 제외하고) 이들 저에너지 방사성 핵을 취급할 때, (전자들의 자기 흡수로 인해) 고체들 중에서 방출된 전자들의 한정된 범위 때문에, 방사성 물질의 매우 얇은 층만이 외부에서 활성적이다, 즉 물질로부터 방출되는 전자들은 매우 얇은 층에서만 생성된다는 것에 유의해야 한다. 예를 들어, ^{63}Ni는 물질의 두께 증가와 무관하게 약 20 mCi/cm^{2}의 최대 표면 방사능을 갖는데 - Belghachi et al. (2020) 참조 - 이러한 물질의 약 10 미크론만이 외부 방사능과 관련이 있다. 1 Ci는 약 $3.7 \cdot 10^{10}$ decay/sec와 같기 때문에, 20 mCi/cm^{2}의 한계는 약 $7.4 \cdot 10^{8}$ decay/(cm^{2} · sec) 또는 10^{9} decay/(cm^{2} · sec)보다 약간 작은 것에 해당함에 주목하자. 이는 ^{63}Ni를 기초로 한 잠재적인 온칩 난수 생성기가 검출기 영역의 1cm^{2}로부터 최대 10억 비트/초를 생성할 수 있으며, 보다 많은 영역이 다른 전자장치에 의해 점유됨을 시사한다. 트리튬 베타 붕괴의 저에너지는 활성층의 두께를 여기서 고려되는 다른 순수한 베타 붕괴 방사성 핵종들의 경우보다 훨씬 더 얇게 되게 하며, 그래서 면적당 생성되는 최대 비트 수가 더 적어진다. 반면에, 주어진 핵종의 반감기는 시간 단위당 방출되는 전자들의 총 개수를 제한한다. 예를 들어, ^{63}Ni의 원자가 100억개, 즉 10^{10}개 있으면, 98.7년 동안 절반만, 즉 초당 약 2개가 붕괴된다. 매우 긴 반감기를 갖는 ^{14}C 방사성 핵종의 경우, 이는 시간 단위당 가능한 총 방사능을 심하게 제한하는데: 초당 2회의 붕괴를 얻기 위해서는 약 1조 또는 10^{12}개의 ^{14}C 원자를 필요로 하며, 즉 니켈 63의 경우와 동일한 방사능을 위해 100배 더 많은 탄소 14 핵이 필요하다. 다시 말하면, 탄소 중의 45 keV 전자들(평균 에너지)의 범위는 니켈 중의 17 keV 전자들(평균 에너지)의 범위보다 겨우 약 8배 더 크기 때문에 초당 동일한 유효 붕괴 횟수를 얻기 위해서는 약 12배 더 넓은 방사성 물질 면적이 필요하다 - Berger 및 Seltzer(1982) 참조(유효층은 8배 더 두꺼울 수 있음). 따라서, ^{63}Ni는 온칩 난수 생성기들의 엔트로피 소스로서 방사성 물질의 표면당 효율의 스위트 스폿에 있는 것으로 보인다. 하지만, 그 최대 방사능은 소위 검출기 반응 데드 타임(dead time)으로 인해 너무 큰 검출기들을 사용할 수 없기 때문에 칩 상에서 생성될 수 있는 비트 수를 여전히 제한한다. 검출될 수 있는 펄스들 사이의 최단 시간은 검출기의 저정전 용량 - 이 정전 용량은 검출기 면적에 비례하여 증가함 - 에 의존한다. 당사의 미국 특허 제11,036,473호에서는, 위에서 언급한 한계를 극복하기 위해 적용될 수 있는 소형 검출기들의 어레이를 사용하는 것을 제안하였다. 여기서는 이러한 접근법과 관련된 문제들을 설명하고 이들 문제를 해결하기 위한 방법들을 제시한다.

[0058] 광자들 또는 전자들의 방출(알려진 순수한 양자 프로세스들)과 같은 자연 현상을 기반으로 하는 모든 난수 생성기들의 주된 문제는 엔트로피 소스의 안정성이다. 광자 기반의 디바이스들의 경우에, 광자들의 소스는 다른 요인들 중에서도 온도, 공급 전압, 및 발광체(다이오드 또는 레이저)의 장기 안정성에 크게 의존한다. 핵 내부의 약한 상호작용에 기인하는 베타 붕괴의 경우, 붕괴의 타이밍이나 방향에 대한 (중력 또는 전자기와 같은) 외부의 장(fields)의 영향은 없다. 절대 영도에 가까운 매우 낮은 온도에서 및 매우 높은 자기장에서만 이들 붕괴는 이방성 또는 소위 패리티 위반(parity violation)을 나타낸다 - 1957년 노벨상 참조. 통상적인 상태에서의 방사성 핵종 엔트로피 소스의 안정성에 대한 유일한 영향은 시간적으로 붕괴 횟수를 줄이는 그 자체의 반감기이다. 위에서 언급한 바와 같이, ^{63}Ni의 경우 반감기는 약 98.7년이다. 시간적으로 붕괴 횟수를 지배하는 지수 방정식, $N=N_0 \cdot e^{-\lambda t}$(N은 $\lambda=\ln(2)/t_{1/2}$로 시간 t 후에 초기 개수 N_0로부터 남은 원자들의 개수이며, 여기서 $t_{1/2}$는 반감기임)에 따르면, 2년 후에도 여전히 니켈 63 방사성 원자들의 98.6 %가 남게 되는데, 즉 처음에는 니켈 방사능이 연간 0.7 % 미만만이 감소하게 된다. 이는 미국 특허 제11,036,473호에 언급된 자가 교정 프로세스에 의해 용이하게 수정될 수 있다(독출 시간의 변경).

[0059] ^{63}Ni 엔트로피 소스로 초당 10억, 즉 10^9 비트를 생성하는 데 필요한 소형 검출기의 개수를 간단히 추정해보자. 11 미크론의 개별 검출기 반경과 15 mCi/cm^{2}의 방사능을 갖는 엔트로피 소스를 가정하면, 검출기 면적당 초당 약 527 카운트를 얻는다. 초당 1,000회의 속도로 독출하는 1,024개의 검출기는 (당사의 미국 특허 제11,036,473호에 따라) 초당 100만 비트의 수를 제공한다. 하지만, (PIN, SPAD, 또는 APD 다이오드와 같은) 다이오드 검출기들은 CCD 카메라들의 픽셀들과 달리, 전하를 수집할 수 없으며 카운트를 유지하기 위해 추가의 간단한 메모리 회로들과 독출 라인들(readout lines)을 필요로 한다.

[0060] 검출기의 임의의 전자 충돌(electron hits)을 등록하는 데 필요한 간단한 셀(5)이 도 1에 제시되어 있다. 셀(5)은, 증폭기(15)에 연결되고 검출 이벤트를 저장하기 위한 메모리(20)에 연결된 검출기(10)를 갖는 실리콘 기판(8)으로 구성된다. 증폭기(15)는 전자가 검출기(10)에 충돌할 때 검출기(10)에 의해 생성되는 펄스를 증폭하고, 출력에 기록 버퍼를 갖는다. 이 버퍼는 전자가 검출되면 메모리(20)에 "1"을 기록한다. 동일한 검출기에서의 후속 검출 이벤트들은 메모리 셀의 상태를 변경시키지 않는다. 그래서, 메모리 셀은 0 또는 1 - 하나의 랜덤 비트에 상응함 - 만을 포함할 수 있다. 셀(5)은 시그널링될 때 메모리(20)로 하여금 비트 라인(35) 상에서 그 콘텐츠를 리포트하게 하는 워드 라인(25)을 가질 수 있다. 리셋 라인(30)은 셀의 그 메모리를 클리어하여 셀을 다른 검출 기간에 대비한다.

[0061] 도 2는 n개의 셀(5) - 각각 아래에 그 처리 셀을 가짐 - 의 선형 어레이(40)의 배치를 나타낸다. 이 선형 어레이(40)가 워드 라인(25) 상에서 "1"로 선택되면, 어레이 내의 모든 셀들(5)의 상태는 독출되어 비트 라인들(35)을 통해 출력 버퍼/메모리(55)에 저장된다. 출력 버퍼/메모리(55)의 새로운 콘텐츠는 이전 콘텐츠를 대체한다. 독출 시간은 클럭(50)에 의해 제어된다. 선형 어레이(40) 내의 모든 셀들(5)의 상태들이 출력 버퍼(55)에 저장되면, 이 선형 어레이(40) 내의 셀들(5)의 상태들은 리셋 라인(30) 상의 리셋 신호 "1"을 통해 "0"으로 리셋되는데; 이들 기능은 신호 관리를 다루기 위해 클럭(50)을 사용하는 제어 블록(45)에 의해 수행된다. 이러한 선형 어레이(40)는 1밀리초마다 n개의 랜덤 비트를 생성하게 된다. 이러한 선형 어레이들의 매트릭스로부터 더 많은 비트를 얻으려면, 이들은 도 3에 도시된 바와 같이 배치될 수 있다. 방금 설명한 P개의 선형 어레이(40) - 각각 n 비트를 생성함 - 로 구성된 M x P 셀 어레이 매트릭스(65)는 밀리초마다 M x P x n 비트를 생성하게 된다. M x P 셀 어레이 매트릭스(65)는 진성 난수들의 어레이를 생성할 수 있고, 이 어레이를 암호화 클라이언트(115)(도 9 및 도 10 참조)에 제공할 수 있으며, 그리고 나서 전달된 진성 난수를 메모리로부터 삭제할 수 있다.

[0062] 도 3에서와 같이 모든 비트가 개별적으로 출력에 전송되어야 하는 경우, 칩당 비트 수는 정전 방전 보호 회로 및 출력 본딩 패드에 필요한 (예를 들면, 50 x 400 마이크로미터 이상과 같은) 넓은 면적에 의해 심하게 제한된다. 이 제한을 극복하기 위해, 랜덤 출력 비트들(60)은 도 4에 나타낸 바와 같이, 시리얼 인터페이스 회로들(70)을 사용하여 출력들에 시리얼로 전송될 수 있다. 이들 회로(70)의 작동은 독출 시간보다 짧은 시간에 선형 어레이들(40)로부터 모든 비트들을 전송하기에 충분히 높은 주파수를 갖는 고속 클럭(50B)에 의해 제어되게 된다. 예를 들어, 선형 어레이들(40)이 1밀리초마다 독출되면, 고속 클럭(50B)의 주파수는 선형 어레이들 내의 비트 수를 1밀리초로 나눈 값보다 낮아서는 안 된다(고속 클럭의 각 사이클에서 1비트가 출력에 전송된다고 가정함). 시리얼 인터페이스 회로들(70)을 제어하는 고속 클럭(50) 및 독출 시간을 제어하는 저속 클럭(50A)의 두 클럭 소스 모두는 주파수 분주기(50C)를 사용하여 동기화되게 된다. 다시 말하면, 제어 블록(45)은 워드 라

인 신호(25)를 관리하기 위해 고속 클럭(50B)을 사용하고 리셋 신호(30)를 관리하기 위해 저속 클럭(50A)을 사용하며, 주파수 분주기(50C)는 저속 클럭(50A)과 고속 클럭(50B) 사이의 관계를 유지한다.

[0063] 각 검출기가 각 독출 사이클에서 검출된 전자(들)에 대한 정보를 저장하기 위한 그 자체의 메모리를 갖고 있다는 사실은 설명된 난수 생성기의 자가 교정의 다른 방법을 가능케 한다. 표 1에 주어진 예시적인 계산에서는, 15 mCi/cm^2 방사능을 가진 방사선 소스가 1초 동안 단일의 11 미크론의 원형 검출기에 충돌할 수 있는 평균 약 527개의 전자를 생성할 수 있음을 보여준다. 이렇게 생성된 "0"과 "1"의 개수가 같지 않으면, 당사의 이전 특허에서 제안한 바와 같이 독출을 위한 클럭 속도를 조정하는 대신에, 본 시스템은 각 행의 활성 검출기의 개수를 약간 변경할 수 있다. 예를 들어, 높은 카운팅 레이트(counting rate)로 인해 "1"의 개수가 일관되게 1,000개의 검출기당 평균 550개인 경우, 909개의 검출기만 활성화함으로써, 생성기는 균형잡힌 개수의 "0"과 "1"을 반환한다(909 = 1,000/550 · 500). 이러한 유형의 자가 조정은 양호한 통계적 특성들을 보장하기 위해 자주, 예를 들면 매초 또는 1,000회의 독출 후에 행해질 수 있다. 실제로, 컨트롤러는 검출기들을 "스위치 오프"할 필요는 없으며 - 출력 버퍼/메모리(55)의 비트들에 대해 동등한 조치가 취해질 수 있고: 위에서 설명한 바와 같이 "1"의 카운트가 너무 높으면, 독출이 수행될 때마다 909 비트만이 취해지게 되며(비트 수는 전체 8비트 워드들에서 감소함); 그래서, 909비트가 아니라, 904비트만 사용하게 된다(904 = 909 - MOD[909,8], 여기서 MOD는 모듈로 함수, 즉 주어진 수에 의한 나눗셈의 나머지이다). 밸런싱의 각 조정은 출력 버퍼/메모리(55)로부터 독출되는 비트 수를 약간 변경시키게 된다. 각 선형 어레이 내의 검출기들의 총 개수(또는 카운트의 가능한 총 개수)가 "0"과 "1"의 균형잡힌 카운팅에 필요한 검출기들의 유효 개수보다 많도록 하는 것이 중요하며, 그래서 사용되는 방사성 물질의 유한한 반감기로 인해 카운트의 개수가 감소하는 시간의 수정도 또한 가능하게 한다.

[0064] 다음의 표는 대략적인 계산 또는 추정에 대한 상세사항을 제공하며 ^{63}Ni 및 다이오드들의 어레이를 기초로 한 설계가 이론적으로는 칩의 초당 및 cm^2당 최대 0.6 Gb에 이를 수 있음을 보여준다.

표 1

[0065]

단일 검출기(10)	
픽셀의 크기	11 미크론의 원형 검출기에 대해 $9.5 \cdot 10^{-5}$ mm^2
^{63}Ni 소스 방사능	15 mCi/cm^2
픽셀 면적당 방사능	$1.4 \cdot 10^{-5}$ mCi
추정 카운트	527 카운트/초; 참조: $3.7 \cdot 10^{10}$ decays/sec = 1 Ci
검출기들의 라인 어레이(40, 40A)	
라인	1,024 픽셀
사용 면적	측면의 1 미크론의 경계 포함하여0.0015 cm^2
독출 빈도수	1048 fps
생성된 비트 수	$1.1 \cdot 10^6$/초
라인 어레이들의 매트릭스(65)	
32 x 32 라인의 매트릭스	
1,024 라인	1.51 cm^2
연결부	0.20 cm^2; 각각 50 μm x 400 μm
총 면적	1.71 cm^2
총 비트 수	**$6.4 \cdot 10^8$/(second · cm^2)**

[0066] 모든 검출기들을 사용하지만 샘플링 시간을 변경하는 자가 교정의 다른 방법이 당사의 이전 미국 특허 제11,036,473호에 기재되어 있다. 이 접근법에서, 전자들은 주어진 시간에, 전형적으로는 1밀리초에 검출기들의 어레이(예를 들면, 32 x 32, 즉 총 1,024개의 검출기)에 충돌한다.

[0067] 이전 섹션들에서 설명되고 표 1에 요약된 바와 같은, 핵 물리학 기반의 계산들은 한 사이클에서 여러 개의 전자가 동일한 검출기에 충돌할 수 있으며 그래서 이 사이클에서 생성되는 "1"의 개수를 저감시킬 수 있다는 단순한

사실을 고려하지 않는다. 복수의 전자가 동일한 검출기에 충돌할 확률은 무시할 수 있을 정도로 작지는 않다. 1,024개의 검출기와 가변 개수의 전자를 가정한 Monte-Carlo(몬테카를로) 시뮬레이션이 도 5에 도시되어 있다. "관찰된 검출들"은 적어도 하나의 전자 충돌을 등록한 검출기들의 개수인 한편, "필요한 붕괴들"은 "관찰된 검출" 값들을 얻기 위해 생성되어야 하는 전자들의 개수이다. 예상대로, 프로세스는 비선형인데, 즉 "1"의 개수가 증가함에 따라, 이미 충돌된 검출기에 충돌한 확률이 높아진다. 예를 들어, (1,000회의 시뮬레이션에서) 평균 527개의 전자는 검출기들과 연관된 411개의 메모리 상태만을 변경하게 된다. 이는 수정을 초래하는데: 앞서 추정된 1,000 마이크로초 대신에, 이러한 어레이는 약 710개의 생성된 전자 또는 710/527 = 1,347 마이크로초(약 35% 더 긺)를 필요로 하며, 그래서 표 1에서와 같은 검출기들의 시스템의 잠재적 수율을 칩의 초당 및 cm^2 당 약 0.5 Gb로 저하시키게 된다. 이러한 조정들을 자동화하기 위해서는, (도 5에 제시된 것과 같은) 시뮬레이션된 데이터를 사용하고 이를 룩업 테이블로 변환하거나, 주어진 지오메트리 및 기술에서 획득된 실험 데이터로부터 이러한 테이블을 생성해야 한다. 룩업 테이블이 칩에 저장되면, 알고리즘식 접근법은 본 출원에 기재된 다른 시간 관련 현상도 처리하는 자가 교정을 가능하게 한다.

[0068] 생성된 난수 중의 0과 1의 개수 사이의 적절한 균형, 즉 비트 수의 절반은 0이고 나머지 절반은 1이 되는 것은 도 6 및 도 7에 도시된 방식으로 달성될 수도 있는데: 이는 클럭 주기를 필요 이상으로 길게 만든다. 적절한 개수의 "1"을 획득하고 "1"의 개수가 적절한 값(1,024개의 검출기의 예에서는, 이는 512개가 "1"로 카운트되는 것임)에 이르면 센서들로부터의 펄스들의 저장(즉, "1"의 수집)을 중지하는 것. 도 6은 메모리(20)로의 출력을 갖는 증폭기(15)에 연결된 검출기(10)를 포함하여, 도 1을 참조하여 설명된 셀(5)과 동일한 컴포넌트들 중 일부를 갖는 셀(5A)을 도시한다. 셀(5A)은 앞서 설명된 동일한 기능들을 갖는 워드 라인(25), 리셋 라인(30), 및 비트 라인(35)도 또한 갖는다. 선형 어레이(40A)(도 7 참조) 내의 셀들(5A) 각각에 대해 증폭기(15)에 의해 증폭된 검출기(10)로부터의 전기 신호들은 OR 게이트(75)를 통해 카운터(80)로 지향되는데, 카운터(80)는 독출 기간(즉, 리셋 신호들 사이의 시간) 동안 사전 결정된 개수의 "1"이 획득되면 정지 신호(82)를 제어 블록(45)에 송신한다. 위에서 언급한 바와 같이, 1,024개의 셀의 선형 어레이의 예에서는, 이는 512개가 된다.

[0069] 정지 신호(82)가 제어 블록(45)에 주어지면, 제어 블록(45)은 다음으로 워드 라인(25) 신호를 발행하여 셀들의 메모리(20)를 출력 버퍼/메모리(55)에 덤프하고, 리셋 라인(30) 신호를 발행하여 셀들을 리셋한다. 출력 버퍼/메모리(55)는 다음으로 진성 난수를 생성하기 위해 독출될 수 있으며, 그 수는 암호화 클라이언트(115)에 전달될 수 있다. 또한 도 6에는 독출 기간 내에 동일한 셀(5A)로부터의 하나 초과의 펄스를 카운트하는 것을 방지하는 - 이러한 펄스들이 발생하는 경우 - 전송 게이트(72)가 도시되어 있다. 하나의 펄스가 수신되면, 메모리(20)에 "1"이 저장된다. 전송 게이트(72)는 증폭기(15)로부터의 입력, OR 게이트(75)로의 출력, 및 전송 게이트 제어 신호(74)를 위해 메모리(20)로부터 입력되는 하나의 제어 신호를 갖는 스위치로서 기능한다. 입력으로부터 출력으로의 데이터 흐름은 전송 게이트 제어 신호(74)에 의해 제어된다. 전송 게이트(72)는 "0" 비트가 메모리(20)에 저장될 때 열리고(CTR = "0") "1"이 거기에 저장될 때(CTR = "1") 닫히며; 그래서 셀 내의 검출기(10)가 이미 전자의 검출을 등록했을 때 전송 게이트(72)는 닫힌다("1"이 메모리(20)에 저장되게 한다). 다른 전자가 동일한 셀 내의 검출기(10)에 충돌하면, 추가 펄스는 전송 게이트(72)를 통해 OR 게이트(75)로 및 궁극적으로 카운터(80)로 전송되지 않는다. 동일한 독출 기간 동안 셀(5A)로부터의 후속 검출들은 카운터(80)에 리포트되지 않으며, 그래서 메모리에는 하나의 "1"만 저장되는 동안 카운터(80)가 2개의 "1"을 잘못 카운트하는 것을 방지한다. 정지 신호(82)를 송신한 후, 카운터(80)는 자체를 리셋할 수 있다. 혹은, 카운터는 계속될 수 있으며 사전 결정된 수치의 배수에 이르렀을 때 정지 신호(82)를 송신하도록 구성될 수 있다.

[0070] 전술한 셀 어레이 매트릭스로 칩을 구성할 때, 독출, 메모리, 및 처리 회로는 베타 방사선으로 인한 방사선 손상으로부터 보호되어야 한다. 이 보호를 달성하는 한 가지 방법은 전자들을 검출기들의 방향으로만 시준하고 그 측면들로는 시준하지 않는 두꺼운 마스크로 방사선 소스를 덮는 것이다. 하지만, 이러한 마스크는 제조(작고 두꺼운 그리드) 및 셀 어레이 내의 검출기들과 정렬하기가 쉽지 않다. 기술적으로 실행 가능한 해법은 독출, 메모리, 및 처리 회로를 각 검출기 아래(예를 들면, Si 웨이퍼의 타측에)에 배치하는 것이다. 도 8a는 셀 어레이 매트릭스(85), 칩 커버/인클로저(90) 및 방사성 소스(95)(양자 모두 검출기들(5, 5A)의 어레이가 보일 수 있도록 반투명하게 됨)를 포함하는 TRNG 검출기 칩을 도시한다. 도 8b는 도 8a의 어레이 매트릭스로부터의 단일 검출기 셀을 갖는 검출기 칩의 일부의 단면도이다. 이 단면도는 검출기(10)로부터 공동(100)에 의해 분리된, 칩 커버/인클로저(90) 및 방사성 소스(95)(선호되는 소스는 방사성 니켈임)를 도시한다. 처리 회로(110)는 실리콘 기판(8)의 관통 실리콘 비아 연결부들(through silicon vias: TSV)(105)에 의해 검출기(10)에 연결되며, 그래서 처리 회로(110)를 베타 방사선, 즉 방사성 소스에 의해 방출되는 전자들로부터 보호한다. TSV의 두께는 처리 회로(110)의 보호를 최적화하도록 선택될 수 있다. TSV는 예를 들면, Knechtel J. et al.

2017에 기재되어 있다. Si 웨이퍼는 10 미크론 초과의 총 두께를 가지며 그래서 방사성 소스(95)에 의해 방출되는 모든 전자들은 그에 흡수되게 된다. 처리 회로(110)는 검출기(10)의 하류에 있는 전술한 처리 컴포넌트들의 전부 또는 일부를 포함할 수 있고, 증폭기(15), 메모리(20), 제어 블록(45), 클럭(50), 출력 버퍼/메모리(55), 시리얼 인터페이스(70), 전송 게이트(72), OR 게이트(75), 카운터(80), 및/또는 암호화 클라이언트(115)(선택적으로 IC에 있을 수도 있음)를 포함할 수 있다. 메모리(20)는 예를 들면, 이 특수 IC가 장착된 디바이스의 통신 채널들(즉, 암호화 클라이언트(115))의 보안성 랜덤 암호화에 또는 시뮬레이션, 모델링, 및 게이밍에 필요한 랜덤 프로세스들에 온디맨드로 필요한 바이트(비트) 수를 공급할 수 있다.

[0071] 도 9는 셀(5)을 사용하여 집적 회로에 배치될 수 있는 다양한 컴포넌트들의 흐름도이다. 마찬가지로, 도 10은 셀(5A)를 사용하여 집적 회로에 배치될 수 있는 다양한 컴포넌트들의 흐름도이다. 도 8b, 도 9a, 및 도 9b는 방사선 소스(95)(바람직하게는 방사성 니켈), 셀들(5, 5a)의 선형 어레이들(40, 40a)로부터 방사성 니켈을 분리하는 공동(100)을 둘러싸는 인클로저(90)를 갖는 TRNG(85)를 도시한다. 셀들은 방사성 니켈의 붕괴로부터 공동 내의 전자들을 검출하고 검출된 전자들에 대한 신호를 발생시키도록 구성된 검출기(10)를 갖는 실리콘 기판(8)을 포함한다. 검출기(10)에 연결된 증폭기(15)는 신호를 증폭하여 이를 저장을 위해 메모리(20)로 전달한다. 제어 블록(45)은 선형 어레이(40, 40a)의 각 셀(5, 5a)에 연결되고, (a) 각 셀(5, 5A)에 워드 라인 신호(25)를 송신하여, 메모리(20)가 비트 라인(35)을 통해 출력 버퍼/메모리(55)에 그 콘텐츠를 리포트하게 하며; 또한 (b) 각 셀(5, 5A)에 리셋 신호(30)를 송신하여, 메모리(20)를 삭제하게 한다.

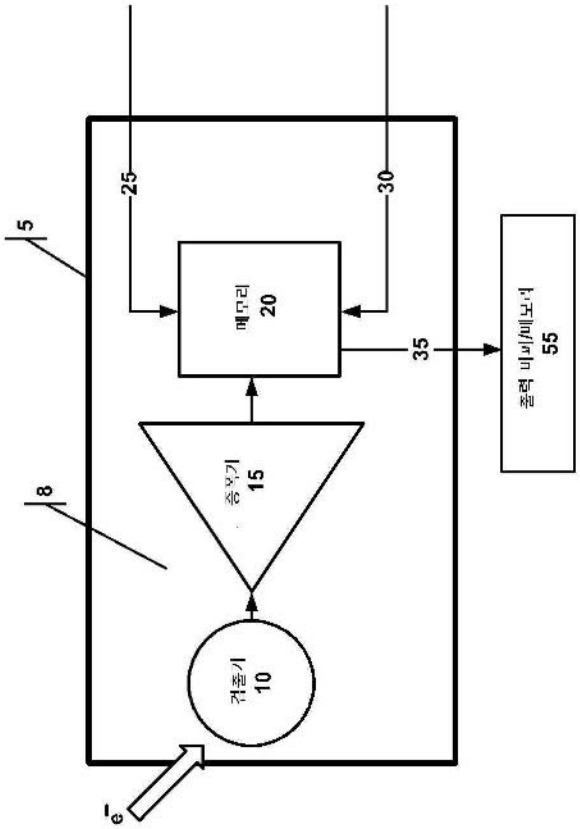
[0072] 본 장치들, 시스템들, 및 방법들의 다양한 예시적인 실시예들은 제조 중에 IC들이 방사성 물질로 함침될 수 있음을 보여준다. 매우 소량의 방사성 니켈로도, 각각의 이러한 칩은 초당 상당한 수의 랜덤 비트를 생성할 수 있다 - 위의 표 1 참조: $6.4 \cdot 10^{8}$ 비트/($s \cdot cm^{2}$). 그 다음에, 이들 비트는 추후 사용을 위해 IC 내부에 통합된 솔리드 스테이트 메모리에 저장될 수 있다. 그래서, 칩 상의 이러한 독립형 TRNG는 (음성 또는 문자 메시지들과 같은) 통신 채널들의 암호화 또는 (시뮬레이션들 또는 게이밍과 같은) 많은 난수를 필요로 하는 프로세스들에 필요한 수천 개의 멀티 바이트 난수를 온디맨드로 쉽게 제공할 수 있다.

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

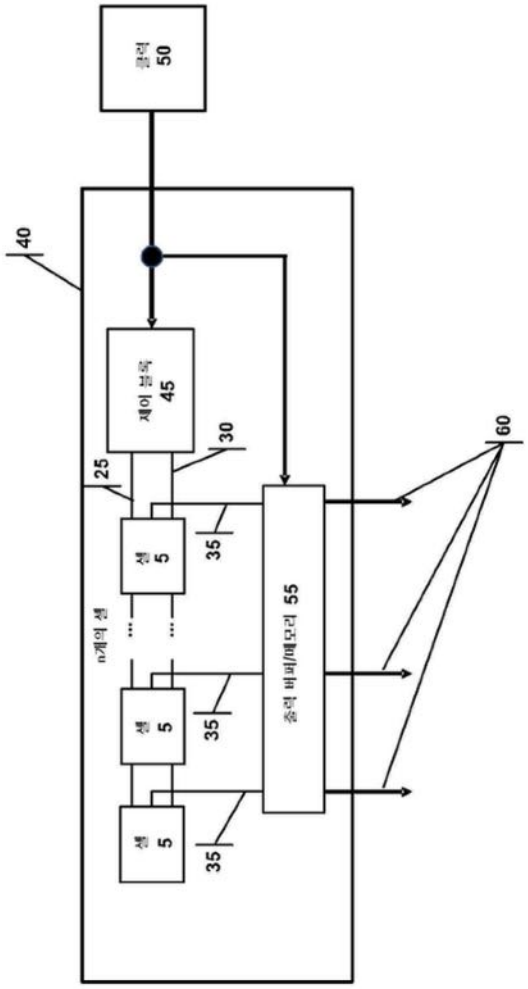
[0074] 본 발명의 예시적인 실시예들과 적용들이 위에서 설명되고 포함된 예시적인 도면들에 도시된 것을 포함하여 본 명세서에 설명되었으나, 본 발명이 이들 예시적인 실시예와 적용에 국한되거나 예시적인 실시예들과 적용들이 동작하거나 본 명세서에 기재된 방식에 국한되는 것을 의도하지는 않는다. 사실, 본 기술분야의 통상의 기술자에게 분명하다시피 예시적인 실시예들에 대한 많은 변경 및 변형이 가능하다. 산출되는 디바이스, 시스템, 또는 방법이 본 특허 출원 또는 임의의 관련된 특허 출원을 기초로 특허청이 허여하는 청구범위 중 하나의 범위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

도면

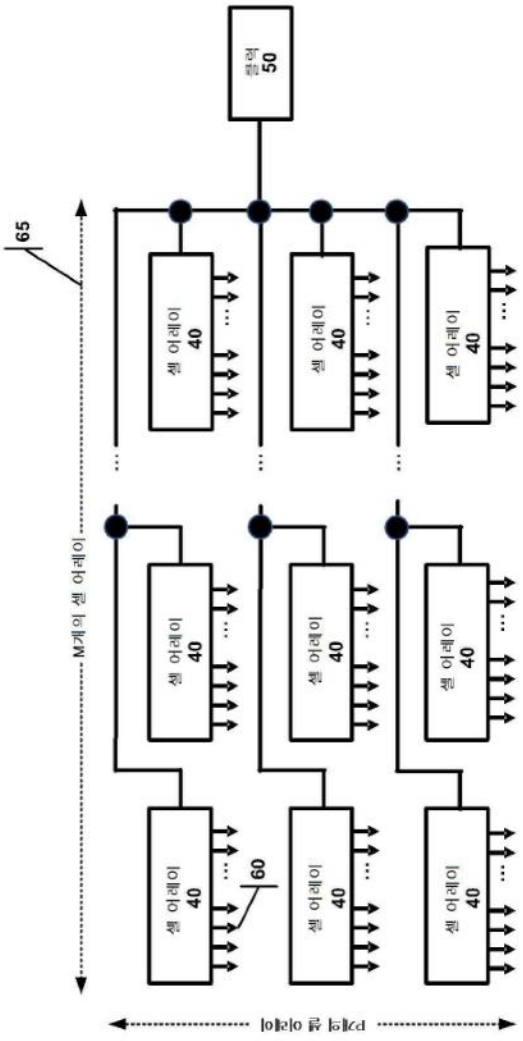
도면1



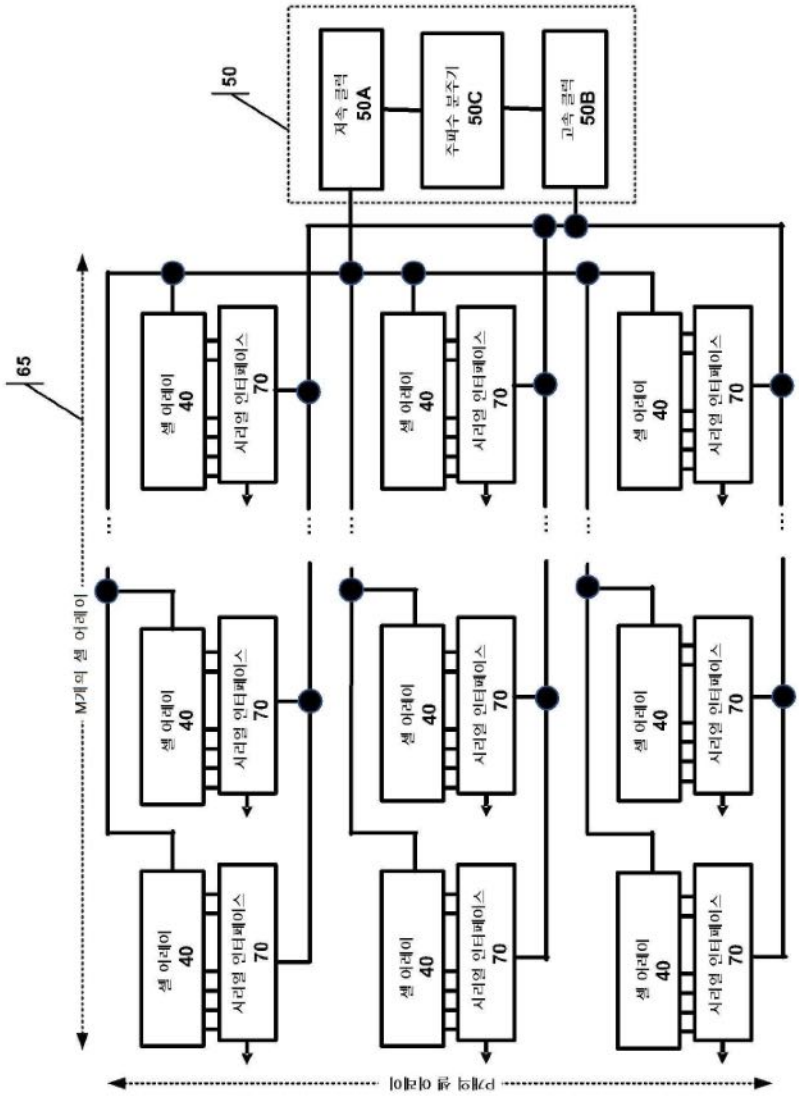
도면2



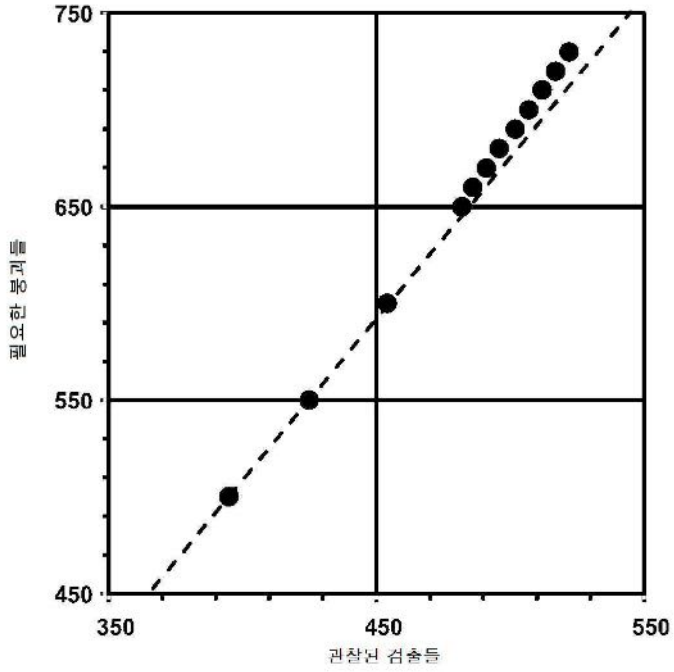
도면3



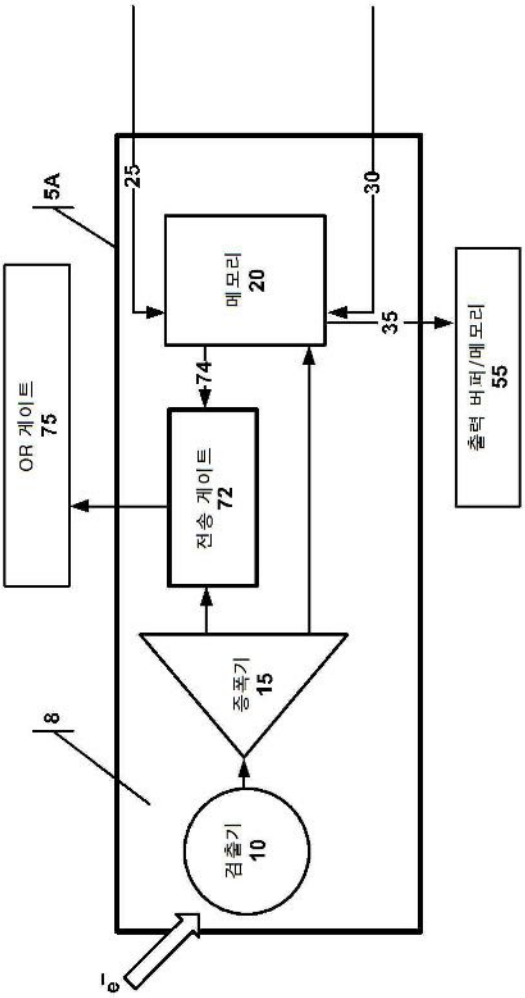
도면4


50
저속 클럭
50A
주파수 분주기
50C
고속 클럭
50B
65
M개의 셀 어레이
N개의 셀 어레이
셀 어레이
40
시리얼 인터페이스
70

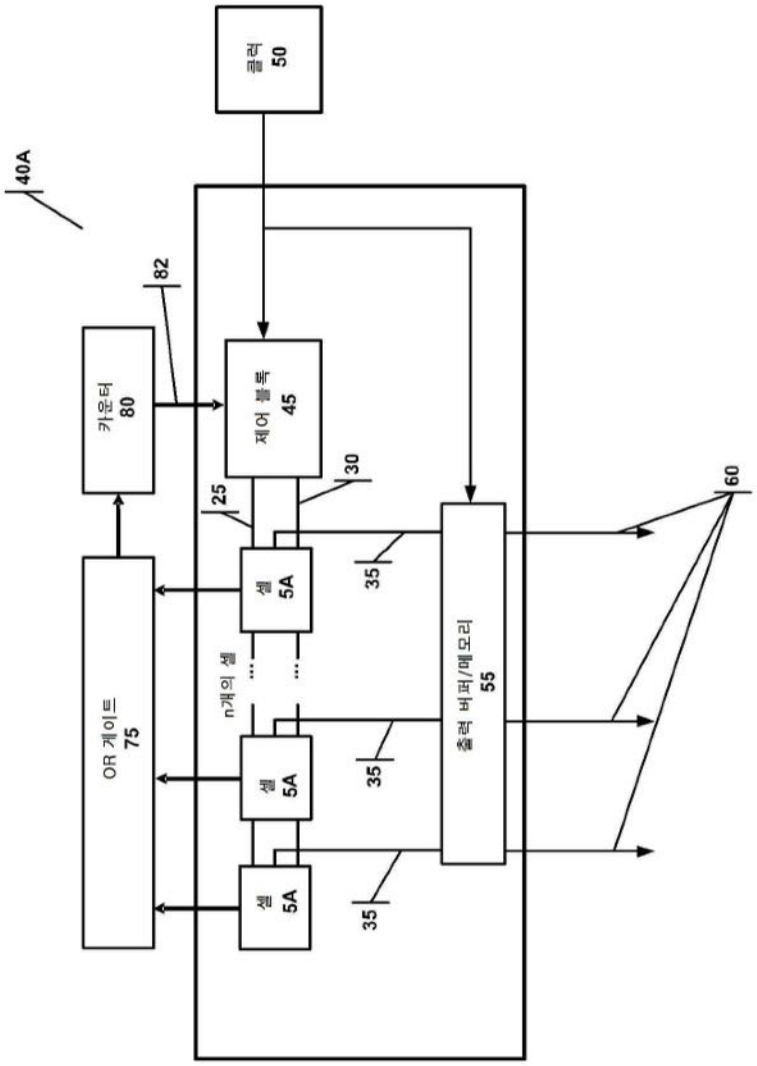
도면5



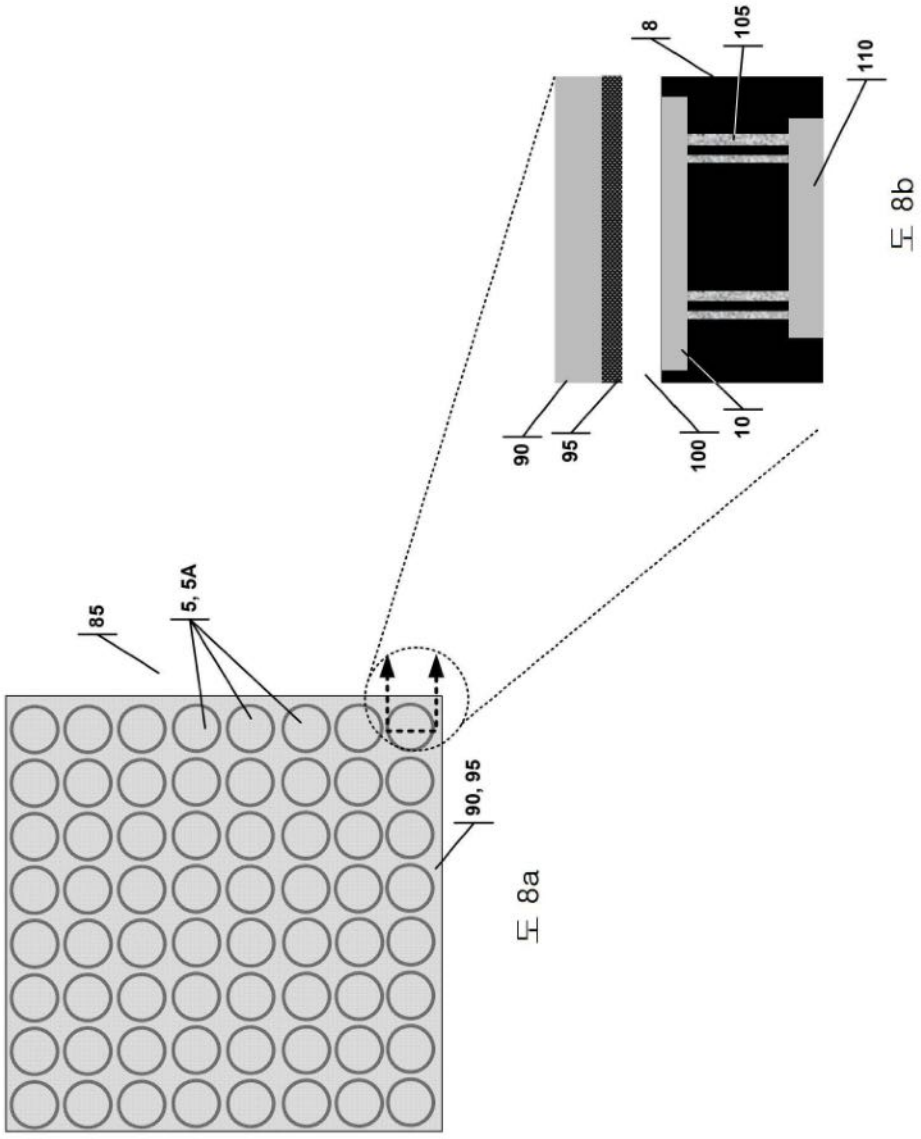
도면6


5A
25
30
메모리
20
35
출력 버퍼/메모리
55
74
OR 게이트
75
전송 게이트
72
증폭기
15
8
검출기
10
I_e

도면7


클럭
50
40A
82
카운터
80
제어 블록
45
30
25
60
셀
5A
35
n개의 셀
OR 게이트
75
출력 버퍼/메모리
55

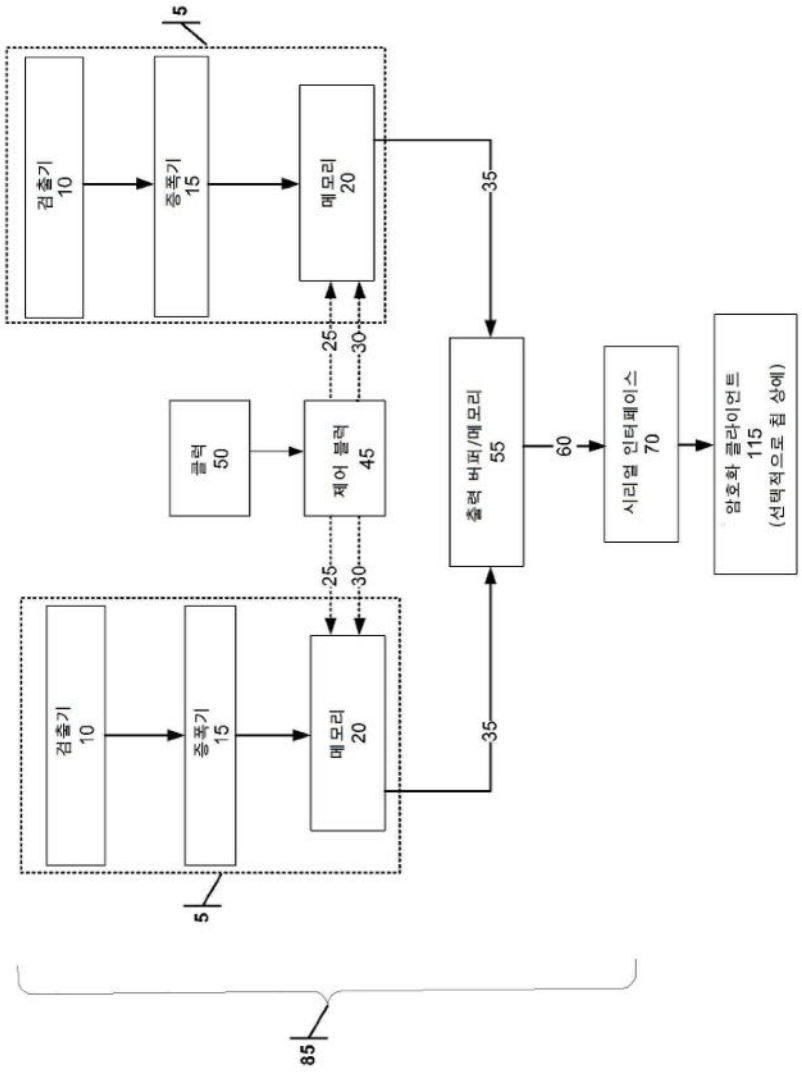
도면8



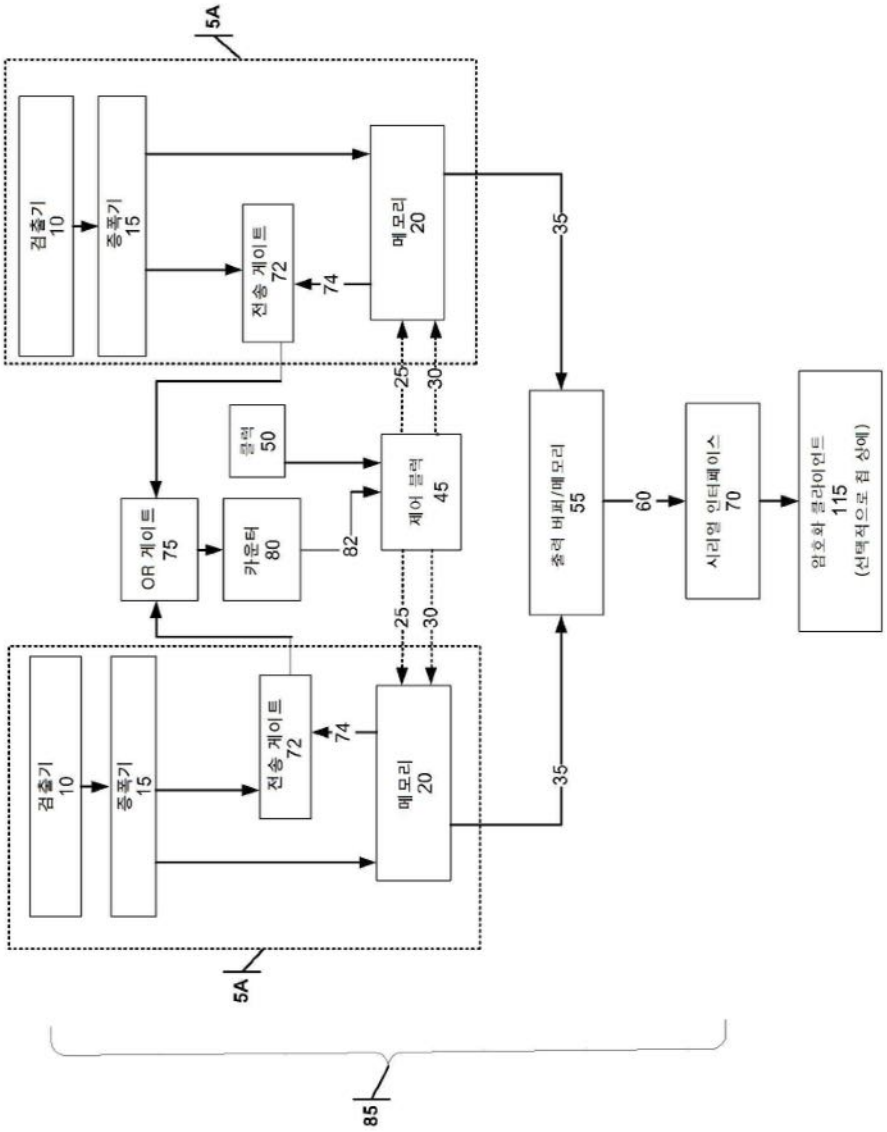
도 8b

도 8a

도면9


5
검출기
10
증폭기
15
메모리
20
35
25
30
클럭
50
제어 블럭
45
출력 버퍼/메모리
55
60
시리얼 인터페이스
70
암호화 클라이언트
115
(선택적으로 칩 상에)
25
30
검출기
10
증폭기
15
메모리
20
35
5
85

도면10


5A
검출기
10
증폭기
15
전송 게이트
72
74
메모리
20
35
25
30
클럭
50
OR 게이트
75
카운터
80
82
제어 블럭
45
출력 버퍼/메모리
55
60
시리얼 인터페이스
70
업호화 클라이언트
115
(선택적으로 접 상에)
85