(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0057531
(43) 공개일자 2020년05월26일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *G06F 21/73* (2013.01)
H03K 3/03 (2006.01)
(52) CPC특허분류
H04L 9/0866 (2013.01)
G06F 21/73 (2013.01)
(21) 출원번호 10-2018-0142041
(22) 출원일자 2018년11월16일
심사청구일자 없음

(71) 출원인
한국전자통신연구원
대전광역시 유성구 가정로 218 (가정동)
(72) 발명자
이상재
대전광역시 유성구 엑스포로 448, 204동 802호(전민동, 엑스포아파트)
오미경
대전광역시 유성구 노은로426번길 15, 603동 1602호(하기동, 송림마을6단지아파트)
(뒷면에 계속)
(74) 대리인
성병기

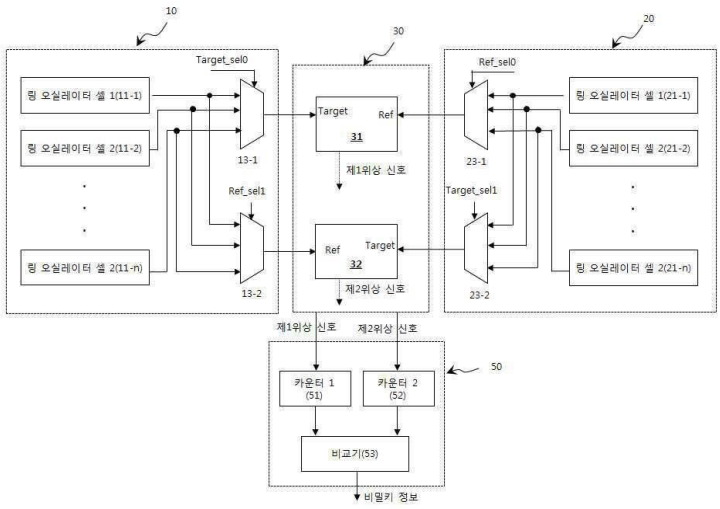
전체 청구항 수 : 총 11 항

(54) 발명의 명칭 **링 발진기 구조 기반의 비밀 정보 생성 장치 및 방법**

(57) 요 약

링 오실레이터 기반의 비밀 정보 생성 장치가 개시된다. 본 개시의 일 실시 예에 따른 링 오실레이터 기반의 비밀 정보 생성 장치는 적어도 하나의 링 오실레이터 셀(ring oscillator cell)을 구비하며, 상기 적어도 하나의 링 오실레이터 셀에 의해 생성되는 PUF(Physically Unclonable Function) 정보를 각각 생성하는 복수의 PUF 정보 생성부와, 상기 복수의 PUF 정보 생성부로부터 각각 출력되는 상기 복수의 PUF 정보에 대한 위상을 교차 확인하는 위상 확인부와, 상기 위상 확인부로부터 제공되는 복수의 위상을 비교한 결과에 기초한 비밀키 정보를 출력하는 비밀키 생성부를 포함할 수 있다.

대 표 도



(52) CPC특허분류
H03K 3/0315 (2013.01)
(72) 발명자
강유성
대전광역시 유성구 대덕대로 598, 803호(도룡동, 더포엠2)
김익균
대전광역시 유성구 대덕대로 594, 904호(도룡동, 타워코리아나 주상복합)
최두호
충청남도 천안시 동남구 용곡2길 43-11, 118동 701호(용곡동, 용곡한라비발디아파트)

이 발명을 지원한 국가연구개발사업
과제고유번호 2018-0-00230
부처명 과학기술정보통신부
연구관리전문기관 정보통신기술진흥센터(IITP)
연구사업명 정보통신방송기술개발사업
연구과제명 (IoT 총괄/1세부) IoT 디바이스 자율 신뢰보장 기술 및 글로벌 표준기반 IoT 통합보안 오픈 플랫폼 기술개발 [TrusThingz 프로젝트]
기 여 율 1/1
주관기관 ETRI
연구기간 2018.04.01 ~ 2021.12.31

명 세 서

청구범위

청구항 1

적어도 하나의 링 오실레이터 셀(ring oscillator cell)을 구비하며, 상기 적어도 하나의 링 오실레이터 셀에 의해 생성되는 PUF(Physically Unclonable Function) 정보를 각각 생성하는 복수의 PUF 정보 생성부와,

상기 복수의 PUF 정보 생성부로부터 각각 출력되는 상기 복수의 PUF 정보에 대한 위상을 교차 확인하는 위상 확인부와,

상기 위상 확인부로부터 제공되는 복수의 위상을 비교한 결과에 기초한 비밀키 정보를 출력하는 비밀키 생성부를 포함하는 것을 특징으로 하는 링 오실레이터 기반의 비밀 정보 생성 장치.

청구항 2

제1항에 있어서,

상기 복수의 PUF 정보 생성부는,

상기 적어도 하나의 링 오실레이터 셀을 구비하며, 제1PUF 정보를 생성하는 제1PUF 정보 생성부와,

상기 적어도 하나의 링 오실레이터 셀을 구비하며, 제2PUF 정보를 생성하는 제2PUF 정보 생성부를 포함하는 것을 특징으로 하는 링 오실레이터 기반의 비밀 정보 생성 장치.

청구항 3

제1항에 있어서,

상기 링 오실레이터 셀은,

오실레이터 인에이블 신호와 시스템 클럭 신호를 입력으로 하는 플립플랍(Flip-Flop) 소자와,

앤드(AND) 게이트와,

상기 앤드 게이트의 출력단에 직렬 연결되는 홀수 개의 인버터 셀과,

상기 홀수 개의 인버터 셀에 구비된 최종 인버터 셀의 클럭을 2분주하는 분주기를 포함하며,

상기 플립플랍 소자의 출력이 상기 앤드 게이트의 제1입력에 연결되고,

상기 최종 인버터 셀의 출력이 상기 앤드 게이트의 제2입력에 연결되는 것을 특징으로 하는 링 오실레이터 기반의 비밀 정보 생성 장치.

청구항 4

제1항에 있어서,

상기 위상 확인부는,

서로 다른 PUF 정보 생성부에서 생성된 PUF 정보를 레퍼런스 신호와 타겟 신호로서 입력받고, 상기 레퍼런스 신호와 타겟 신호 사이의 위상을 검출하여 출력하는 것을 특징으로 하는 링 오실레이터 기반의 비밀 정보 생성 장치.

청구항 5

제2항에 있어서,

상기 위상 확인부는,

상기 제1PUF 정보 생성부가 출력하는 상기 제1PUF 정보를 타겟 신호로서 입력받고, 상기 제2PUF 정보 생성부가 출력하는 상기 제2PUF 정보를 레퍼런스 신호로서 입력받고, 상기 레퍼런스 신호와 타겟 신호 사이의 위상을 검출하여 출력하는 제1위상 처리부와,

상기 제1PUF 정보 생성부가 출력하는 상기 제1PUF 정보를 레퍼런스 신호로서 입력받고, 상기 제2PUF 정보 생성부가 출력하는 상기 제2PUF 정보를 타겟 신호로서 입력받고, 상기 레퍼런스 신호와 타겟 신호 사이의 위상을 검출하여 출력하는 제2위상 처리부를 포함하는 것을 특징으로 하는 링 오실레이터 기반의 비밀 정보 생성 장치.

청구항 6

제1항에 있어서,

상기 비밀키 생성부는,

상기 위상 확인부에서 확인된 상기 복수의 PUF 정보 각각에 대응되는 복수의 위상을 카운팅하는 복수의 카운터와,

상기 복수의 카운터의 출력값을 비교하는 비교기를 포함하는 것을 특징으로 하는 링 오실레이터 기반의 비밀 정보 생성 장치.

청구항 7

제1항에 있어서,

상기 비밀키 생성부는,

상기 제1위상 처리부에서 출력되는 제1위상값을 카운팅하는 제1카운터와,

상기 제2위상 처리부에서 출력되는 제2위상값을 카운팅하는 제2카운터와,

상기 제1 및 제2카운터의 출력을 비교하는 비교기를 포함하는 것을 특징으로 하는 링 오실레이터 기반의 비밀 정보 생성 장치.

청구항 8

적어도 하나의 링 오실레이터 셀(ring oscillator cell)를 구비한 복수의 제PUF(Physically Unclonable Function) 정보 생성부가, PUF 정보를 생성 및 출력하는 과정과,

상기 복수의 PUF 정보 생성부로부터 각각 출력되는 상기 복수의 PUF 정보에 대한 위상을 확인하는 과정과,

상기 복수의 PUF 정보에 대응되는 복수의 위상을 각각 카운트한 값을 비교하여 비밀키 정보를 생성하는 과정을 포함하는 것을 특징으로 하는 링 오실레이터 기반의 비밀 정보 생성 방법.

청구항 9

제8항에 있어서,

상기 PUF 정보를 생성 및 출력하는 과정은,

상기 적어도 하나의 링 오실레이터 셀을 사용하여 제1PUF 정보를 생성하는 과정과,

상기 적어도 하나의 링 오실레이터 셀을 사용하여 제2PUF 정보를 생성하는 과정을 포함하는 것을 특징으로 하는 링 오실레이터 기반의 비밀 정보 생성 방법.

청구항 10

제8항에 있어서,

상기 위상을 확인하는 과정은,

서로 다른 PUF 정보 생성부에서 생성된 PUF 정보를 레퍼런스 신호와 타겟 신호로서 입력받고, 상기 레퍼런스 신호와 타겟 신호 사이의 위상을 검출하는 과정을 포함하는 것을 특징으로 하는 링 오실레이터 기반의 비밀 정보 생성 방법.

청구항 11

제8항에 있어서,

상기 비밀키 정보를 생성하는 과정은,

상기 확인된 상기 복수의 PUF 정보 각각에 대응되는 복수의 위상을 각각 카운팅하는 과정과,

상기 카운팅된 값을 비교하여 비밀키 정보를 생성하는 과정을 포함하는 것을 특징으로 하는 링 오실레이터 기반의 비밀 정보 생성 방법.

발명의 설명

기 술 분 야

[0001] 본 개시는 디지털 지문 제공 기술에 관한 것으로, 특히 링 오실레이터 기반의 PUF를 이용하여 하드웨어 IP에 디지털 지문을 구현하는 방법 및 장치에 대한 것이다.

배 경 기 술

[0002] IoT(Internet of Things) 기술의 확산에 따라 수많은 IoT 기기가 개발되고 판매되고 있으며 IoT 기기를 보호하기 위한 소프트웨어적인 보안 기능들이 탑재되고 있다. 특히 IoT 기기에는 기기 고유의 정보를 식별할 수 있는 암호화 key나 식별 정보(ID)를 내장하고 있으나 최근 들어 보안 상의 취약점을 이용하여 key나 ID를 알아내어 공격하는 사례가 다수 보고되고 있다.

[0003] 한편, 물리적 복지 방지 기술(Physical Unclonable Function, PUF)는 디지털 기기의 복제 방지 기술로, 동일한 회로라 하더라도 회로를 구현하는 공정 상황에 따라 선로 지연(wire delay) 및 게이트 지연(gate delay)이 미세하게 다르다는 점을 이용하여 복제 여부를 확인하는 기술이다.

[0004] PUF는 작은 게이트 로직으로 구현 가능하며, 랜덤 출력을 쉽게 생성할 수 있는 특징이 있다. 또한 PUF 회로는 회로 구조가 동일한 셀들로 구성되고, 같은 제조 공정으로 만들어 지지만, 제조 공정 편차에 따라 셀들이 미세하게 서로 다른 값들을 출력한다.

[0005] 즉, PUF는 공정 상황에 따른 지연(delay)의 차이를 이용하므로, PUF 회로가 공개되더라도, 동일한 출력을 하는 회로의 구성이 어렵다. 이러한 PUF의 특징으로, PUF는 인간의 지문처럼 각 소자 고유의 인식 정보를 생성시키며, 물리적 복제방지 기능을 수행한다. 즉, PUF 회로의 여러 셀들마다 미세한 차이를 검출하여 지문처럼 사용할 수 있다.

발명의 내용

해결하려는 과제

[0006] 나아가, IoT 기기의 보안을 위하여, 설계자 또는 사용자가 IoT 기기 설정을 위한 식별 정보(ID)나, 보안정보(예, password)를 기기 자체에 설정하도록 구비되지만, PUF를 이용할 경우 이러한 설계자 또는 사용자

의 설정없이 기기 자체에 고유한 식별정보나, 보안정보(예, 비밀키 정보)를 생성할 수 있다.

[0007] 본 개시의 기술적 과제는 링 오실레이터 셀을 통해 생성되는 클럭신호의 위상을 검출하고, 검출된 위상신호를 사용하여 비밀 정보를 생성하는 방법 및 장치를 제공하는데 있다.

[0008] 본 개시의 다른 기술적 과제는 서로 다른 링 오실레이터 셀을 통해 생성되는 클럭신호의 위상을 카운트하고, 카운트된 결과를 사용하여 비밀 정보를 생성하는 방법 및 장치를 제공하는데 있다.

[0009] 본 개시에서 이루고자 하는 기술적 과제들은 이상에서 언급한 기술적 과제들로 제한되지 않으며, 언급하지 않은 또 다른 기술적 과제들은 아래의 기재로부터 본 개시가 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0010] 본 개시의 일 양상에 따르면 링 오실레이터 기반의 비밀 정보 생성 장치가 제공될 수 있다. 상기 장치는 적어도 하나의 링 오실레이터 셀(ring oscillator cell)을 구비하며, 상기 적어도 하나의 링 오실레이터 셀에 의해 생성되는 PUF(Physically Unclonable Function) 정보를 각각 생성하는 복수의 PUF 정보 생성부와, 상기 복수의 PUF 정보 생성부로부터 각각 출력되는 상기 복수의 PUF 정보에 대한 위상을 교차 확인하는 위상 확인부와, 상기 위상 확인부로부터 제공되는 복수의 위상을 비교한 결과에 기초한 비밀키 정보를 출력하는 비밀키 생성부를 포함할 수 있다.

[0011] 본 개시의 다른 양상에 따르면 링 오실레이터 기반의 비밀 정보 생성 방법이 제공될 수 있다. 상기 방법은 적어도 하나의 링 오실레이터 셀(ring oscillator cell)를 구비한 복수의 PUF(Physically Unclonable Function) 정보 생성부가, PUF 정보를 생성 및 출력하는 과정과, 상기 복수의 PUF 정보 생성부로부터 각각 출력되는 상기 복수의 PUF 정보에 대한 위상을 확인하는 과정과, 상기 복수의 PUF 정보에 대응되는 복수의 위상을 각각 카운트한 값을 비교하여 비밀키 정보를 생성하는 과정을 포함할 수 있다.

[0012] 본 개시에 대하여 위에서 간략하게 요약된 특징들은 후술하는 본 개시의 상세한 설명의 예시적인 양상일 뿐이며, 본 개시의 범위를 제한하는 것은 아니다.

발명의 효과

[0013] 본 개시에 따르면, 링 오실레이터 셀을 통해 생성되는 클럭신호의 위상을 검출하고, 검출된 위상신호를 사용하여 비밀 정보를 생성하는 방법 및 장치가 제공될 수 있다.

[0014] 본 개시에 따르면, 서로 다른 링 오실레이터 셀을 통해 생성되는 클럭신호의 위상을 카운트하고, 카운트된 결과를 사용하여 비밀 정보를 생성하는 방법 및 장치가 제공될 수 있다.

[0015] 본 개시에 따르면, 서로 다른 링 오실레이터 셀을 통해 생성되는 클럭신호의 위상을 사용하여 비밀키 정보를 생성하므로써, 상대적으로 많은 수의 시도-응답 쌍을 구성할 수 있는 방법 및 장치가 제공될 수 있다.

[0016] 본 개시에서 얻을 수 있는 효과는 이상에서 언급한 효과들로 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

[0017] 도 1은 본 개시의 일 실시예에 따른 비밀 정보 생성 장치의 구성을 도시하는 블록도이다.

도 2는 본 개시의 일 실시예에 따른 비밀 정보 생성 장치에 구비되는 링 오실레이터 셀의 구체적인 구성을 예시하는 도면이다.

도 3a 및 3b는 본 개시의 일 실시예에 따른 비밀 정보 생성 장치에서 사용되는 신호의 타이밍을 나타내는 도면이다.

도 4는 본 개시의 일 실시예에 따른 비밀 정보 생성 장치의 링 오실레이터 셀의 선택에 사용되는 제어신호를 예시하는 도면이다.

발명을 실시하기 위한 구체적인 내용

[0018] 이하에서는 첨부한 도면을 참고로 하여 본 개시의 실시 예에 대하여 본 개시가 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나, 본 개시는 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시 예에 한정되지 않는다.

[0019] 본 개시의 실시 예를 설명함에 있어서 공지 구성 또는 기능에 대한 구체적인 설명이 본 개시의 요지를 흐릴 수 있다고 판단되는 경우에는 그에 대한 상세한 설명은 생략한다. 그리고, 도면에서 본 개시에 대한 설명과 관계없는 부분은 생략하였으며, 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[0020] 본 개시에 있어서, 어떤 구성요소가 다른 구성요소와 "연결", "결합" 또는 "접속"되어 있다고 할 때, 이는 직접적인 연결관계뿐만 아니라, 그 중간에 또 다른 구성요소가 존재하는 간접적인 연결관계도 포함할 수 있다. 또한 어떤 구성요소가 다른 구성요소를 "포함한다" 또는 "가진다"고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 배제하는 것이 아니라 또 다른 구성요소를 더 포함할 수 있는 것을 의미한다.

[0021] 본 개시에 있어서, 서로 구별되는 구성요소들은 각각의 특징을 명확하게 설명하기 위함이며, 구성요소들이 반드시 분리되는 것을 의미하지는 않는다. 즉, 복수의 구성요소가 통합되어 하나의 하드웨어 또는 소프트웨어 단위로 이루어질 수도 있고, 하나의 구성요소가 분산되어 복수의 하드웨어 또는 소프트웨어 단위로 이루어질 수도 있다. 따라서, 별도로 언급하지 않더라도 이와 같이 통합된 또는 분산된 실시 예도 본 개시의 범위에 포함된다.

[0022] 본 개시에 있어서, 다양한 실시 예에서 설명하는 구성요소들이 반드시 필수적인 구성요소들은 의미하는 것은 아니며, 일부는 선택적인 구성요소일 수 있다. 따라서, 일 실시 예에서 설명하는 구성요소들의 부분집합으로 구성되는 실시 예도 본 개시의 범위에 포함된다. 또한, 다양한 실시 예에서 설명하는 구성요소들에 추가적으로 다른 구성요소를 포함하는 실시 예도 본 개시의 범위에 포함된다.

[0023] 이하, 첨부한 도면을 참조하여 본 개시의 실시 예들에 대해서 설명한다.

[0024] 도 1은 본 개시의 일 실시예에 따른 비밀 정보 생성 장치의 구성을 도시하는 블록도이다.

[0025] 도 1을 참조하면, 비밀 정보 생성 장치는 제1 및 제2PUF 정보 생성부(10, 20), 위상 확인부(30), 및 비밀키 생성부(50)를 포함할 수 있다.

[0026] 제1PUF 정보 생성부(10)는 적어도 하나의 링 오실레이터 셀(ring oscillator cell)(11-1, 11-2, ..., 11-n)과, 적어도 하나의 MUX(13-1,13-2)를 구비할 수 있다. 그리고, 적어도 하나의 MUX(13-1,13-2)는 각각 적어도 하나의 링 오실레이터 셀(11-1, 11-2, ..., 11-n)로부터 출력되는 클럭신호를 선택적으로 출력할 수 있다.

[0027] 마찬가지로, 제2PUF 정보 생성부(20)는 적어도 하나의 링 오실레이터 셀(21-1, 21-2, ..., 21-n)과, 적어도 하나의 MUX(23-1, 23-2)를 구비할 수 있다. 그리고, 적어도 하나의 MUX(23-1, 23-2)는 각각 적어도 하나의 링 오실레이터 셀(21-1, 21-2, ..., 21-n)로부터 출력되는 클럭신호를 선택적으로 출력할 수 있다.

[0028] 위상 확인부(30)는 제1 및 제2PUF 정보 생성부(10, 20)에서 출력되는 제1 및 제2PUF 정보 사이의 위상을 교차 확인한다.

[0029] 구체적으로, 위상 확인부(30)는 제2PUF 정보 생성부(20)에서 출력되는 제2PUF 정보를 기준으로, 제1PUF 정보 생성부(10)에서 출력되는 제1PUF 정보의 위상을 확인하는 제1위상 처리부(31)를 포함할 수 있다. 이를 위해, 제1위상 처리부(31)는 제1PUF 정보를 타겟 신호로서 제2PUF 정보를 레퍼런스 신호로서 입력받고, 제1위상 신호를 출력할 수 있다.

[0030] 또한, 위상 확인부(30)는 제1PUF 정보 생성부(10)에서 출력되는 제1PUF 정보를 기준으로, 제2PUF 정보 생성부(20)에서 출력되는 제2PUF 정보의 위상을 확인하는 제2위상 처리부(32)를 포함할 수 있다. 제2위상 처리부(32)는 제2PUF 정보를 타겟 신호로서 제1PUF 정보를 레퍼런스 신호로서 입력받고, 제2위상 신호를 출력할 수 있다.

[0031] 제1 및 제2위상신호는 각각 적어도 하나의 링 오실레이터 셀로부터 출력되는 클럭신호를 기반으로 생성되는 신호일 수 있다.

[0032] 비밀키 생성부(50)는 위상 확인부(30)로부터 제공되는 제1 및 제2위상신호를 비교한 결과에 기초한 비밀키 정보를 출력할 수 있다. 구체적으로, 비밀키 생성부(50)는 제1 및 제2위상신호의 값을 각각 카운팅하는 제1카운터 및 제2카운터(51, 52)를 포함할 수 있다. 또한, 비밀키 생성부(50)는 제1카운터 및 제2카운터(51, 52)의 값을 비교하는 비교기(53)를 포함할 수 있으며, 비교기(53)를 통해 출력되는 결과값을 비밀키 정보로서 생성하여 출력할 수 있다.

[0033] 본 개시의 일 실시예에서, 비밀 정보 생성 장치는 제1 및 제2PUF 정보 생성부(10, 20)를 구비하고, 이에 기초하여 위상 확인부(30)는 제1 및 제2PUF 정보에 대응되는 제1 및 제2위상 신호을 확인하고, 비밀키 생성부(50)는 제1 및 제2위상 신호를 기반으로하는 비밀키 정보를 생성하는 것을 예시하였으나, 본 개시가 이를 한정하는 것은 아니다. 비밀 정보 생성 장치는 복수개의 PUF 정보를 생성하는 복수개의 PUF 정보 생성부를 포함할 수 있으며, 이에 대응하여 위상 확인부(30)와 비밀키 생성부(50)의 구성이 변경될 수 있다.

[0034] 도 2는 본 개시의 일 실시예에 따른 비밀 정보 생성 장치에 구비되는 링 오실레이터 셀의 구체적인 구성을 예시하는 도면이다.

[0035] 도 2를 참조하면, 링 오실레이터 셀(200)은 플립플랍(Flip-Flop) 소자(210), 앤드(AND) 게이트(220), 홀수 개의 인버터 셀(230-1, 230-2, ..., 230-m, m은 홀수), 및 2분주기(240)를 포함할 수 있다.

[0036] 플립플랍 소자(210)는 오실레이터 인에이블 신호를 입력받는 제1입력단(211)과, 시스템 클럭 신호를 입력받는 제2입력단(212)를 포함할 수 있다. 플립플랍 소자(210)의 출력단(213)은 앤드 게이트(220)의 제1입력단(221)에 연결되고, 앤드 게이트(220)의 제2입력단(222)은 홀수 개의 인버터 셀(230-1, 230-2, ..., 230-p, p는 홀수) 중 최종 인버터 셀(230-p)의 출력과 연결될 수 있다.

[0037] 그리고, 최종 인버터 셀(230-p)의 출력은 2분주기(240)로 제공될 수 있으며, 2분주기(240)는 링 오실레이터 셀(200)를 기반으로 생성되는 신호를 2분주하여 출력할 수 있다.

[0038] 한편, 링 오실레이터 셀(200) 각각은 반도체 레벨에서의 제조 환경에 기초하여 형성되는 공진 주파수를 구비하는 클럭신호를 출력할 수 있는데, 클럭신호에 포함되는 공진 주파수는 서로 다르게 형성될 수 있다.

[0039] 그리고, 제1 및 제2PUF 정보 생성부(10, 20)에 각각 구비된 MUX를 통해 링 오실레이터 셀(200)이 각각 선택될 수 있으며, 선택된 링 오실레이터 셀(200)에 대응되는 클럭신호가 출력될 수 있다. 클럭신호는 서로 다른 공진 주파수를 구비할 수 있으므로, 서로 다른 위상을 구비할 수 있다. 따라서, 제1 및 제2PUF 정보 생성부(10, 20)에서 각각 제공되는 클럭신호에 대한 위상을 검출하고, 이를 카운팅한 결과를 비교한 값을 생성할 수 있다. 나아가, 제1 및 제2PUF 정보 생성부(10, 20)에는 각각 복수의 링 오실레이터 셀(200)이 구비될 수 있으므로, 각각의 링 오실레이터 셀(200)에 대한 위상과, 위상을 카운팅한 결과의 비교값을 조합하여 최종적으로 비밀키 정보를 생성할 수 있다.

[0040] 이하, 본 개시의 일 실시예에 따른 비밀 정보 생성 장치의 동작을 구체적으로 설명한다.

[0041] 먼저, 제1위상 처리부(31)에 레퍼런스 신호와 타겟 신호로서 입력될 두개의 클럭신호를 선택하기 위하여, 제1PUF 정보 생성부(10)에 포함된 제1MUX(13-1)에 Target_sel0 신호를 인가하고, 제2PUF 정보 생성부(20)에 포함된 제1MUX(23-1)에 Ref_sel0 신호를 인가한다. 마찬가지로, 제2위상 처리부(32)에 레퍼런스 신호와 타겟 신호로서 입력될 두개의 클럭신호를 선택하기 위하여, 제1PUF 정보 생성부(10)에 포함된 제2MUX(13-2)에 Ref_sel1 신호를 인가하고, 제2PUF 정보 생성부(20)에 포함된 제2MUX(23-2)에 Target_sel1 신호를 인가한다.

[0042] 그리고, 제1PUF 정보 생성부(10)와 제2PUF 정보 생성부(20)에 구비된 적어도 하나의 링 오실레이터 셀에 osc_enable 신호를 인가함으로써, 제1PUF 정보 생성부(10)와 제2PUF 정보 생성부(20)에 구비된 링 오실레이터 셀을 동시에 구동시킬 수 있다.

[0043] 이에 따라, 제1PUF 정보 생성부(10)에 포함된 제1MUX(13-1)에서 출력되는 클럭신호는 제1위상 처리부(31)의 타겟 신호로서 입력되고, 제2PUF 정보 생성부(20)에 포함된 제1MUX(23-1)에서 출력되는 클럭신호는 제1위상 처리부(31)의 레퍼런스 신호로서 입력될 수 있다. 그리고, 제2PUF 정보 생성부(20)에 포함된 제2MUX(23-2)에서 출력되는 클럭신호는 제2위상 처리부(32)의 타겟 신호로서 입력되고, 제1PUF 정보 생성부(10)에 포함된 제2MUX(13-2)에서 출력되는 클럭신호는 제2위상 처리부(32)의 레퍼런스 신호로서 입력될 수 있다.

[0044] 이러한 동작을 통해, 제1위상 처리부(31)는 제2PUF 정보 생성부(20)에서 출력되는 클럭신호를 기준으로 제1PUF 정보 생성부(10)에서 출력되는 클럭신호에 대한 제1위상신호을 검출하여 출력하고, 제2위상 처리부(32)는 제1PUF 정보 생성부(10)에서 출력되는 클럭신호를 기준으로 제2PUF 정보 생성부(20)에서 출력되는 클럭신호에 대한 제2위상신호를 검출하여 출력할 수 있다.

[0045] 비밀키 생성부(50)에 구비된 제1 및 제2카운터(51, 52)는 각각 미리 정해진 시간동안 제1 및 제2위상신호의 값을 카운팅하고, 비교기(55)는 카운팅된 결과를 비교하여 비밀키 정보를 생성할 수 있다.

[0046] 예를 들어, 제1 카운터의 값이 제2카운터의 값과 동일하거나 상대적으로 더 높은값(예, 주파수)으로 확인할 경

우, 비밀키 생성부(50)는 그 결과값을 '1'로 생성할 수 있다. 제1 카운터의 값이 제2카운터의 값보다 상대적으로 더 낮은값(예, 주파수)으로 확인할 경우, 비밀키 생성부(50)는 그 결과값을 '0'으로 생성할 수 있다.

[0047] 도 3a 및 3b는 본 개시의 일 실시예에 따른 비밀 정보 생성 장치에서 사용되는 신호의 타이밍을 나타내는 도면이다.

[0048] 우선, 제1 및 제2PUF 정보 생성부(10, 20)에 구비되는 각각의 링 오실레이터 셀은 클럭신호(osc_clock)(301)를 생성하고, 이를 2분주한 클럭신호(osc_clock/2)(302)로 변환하여 출력할 수 있다. 이때, 제1 및 제2PUF 정보 생성부(10, 20)에 구비된 적어도 하나의 MUX는 2분주한 클럭신호(302)를 선택적으로 타겟 신호 또는 레퍼런스 신호로서 출력할 수 있으며, 타겟 신호 또는 레퍼런스 신호의 출력 선택은 Target_sel0, Tartget_sel1, Ref_sel0, Ref_sel1 등의 제어신호를 사용하여 수행될 수 있다.

[0049] 제1 및 제2PUF 정보 생성부(10, 20)에 구비된 적어도 하나의 MUX를 통해 출력되는 클럭신호($CLK_{target}/2$, $CLK_{ref}/2$)(311, 321)는 교차하여 제1 및 제2위상 처리부(31, 32)에 입력될 수 있다. 제1 및 제2위상 처리부(31, 32)는 타겟 신호 또는 레퍼런스 신호로서 입력된 클럭신호($CLK_{target}/2$, $CLK_{ref}/2$)(311, 321)를 다시 2분주하고, 이 신호($CLK_{target}/4$, $CLK_{ref}/4$)(313, 323)를 이용해서 제1 및 제2위상신호를 검출행한다.

[0050] 클럭신호의 분주율은 실제 구현 시 oscillator의 발진 클럭에 따라 2분주, 4분주, 8분주 등으로 조정될 수 있다. 위상신호의 검출은 4분주된 레퍼런스 신호($CLK_{ref}/4$)(323)의 상승 에지(rising edge)에서 4분주된 타겟 신호($CLK_{target}/4$)(313)가 1이면 검출로 판단하여 위상 검출(phase detection) 신호(330)를 발생시키고 0으로 검출되면 위상 검출(phase detection) 신호를 발생시키지 않는다.

[0051] 위상 검출(phase detection) 신호가 발생되면 그에 대응되는 제1카운터 또는 제2카운터(51, 52)는 카운팅값을 증가시키게 된다.

[0052] 오실레이터(oscillator)의 발진 주파수가 제조 특성에 따라 하드웨어적인 불확실성에 영향을 받아 조금씩의 차이를 가지고 있고 이로 인해 클럭이 달라지므로, 전술한 바와 같이 위상 검출이 가능하게 된다. 이와 같이 검출된 위상을 미리 정해진 시간 동안 누적 카운팅하고, 누적 카운팅된 값을 비교함으로써, 랜덤한 비밀키 정보를 생성할 수 있다.

[0053] 도 4는 본 개시의 일 실시예에 따른 비밀 정보 생성 장치의 링 오실레이터 셀의 선택에 사용되는 제어신호를 예시하는 도면이다.

[0054] 예컨대, 제1 및 제2PUF 정보 생성부(10, 20)가 각각 32개의 링 오실레이터 셀을 구비하면, 비밀 정보 생성 장치에는 전체 64개의 링 오실레이터 셀이 구비될 수 있다. 위상 처리부가 2개가 구비될 경우, 각각의 PUF 정보 생성부에서는 하나의 target과 하나의 reference 링 오실레이터 셀의 선택이 가능하므로 도 4에서 Target0 필드(411) 및 Reference0 필드(415)는 각각 5bit씩 총 10bit로 구성되고, Target1 필드(421) 및 Reference1 필드(425) 역시 각각 5bit씩 총 10bit로 구성되므로, 전체 20bit에 임의의 값을 설정하여 하나의 비밀키 정보(1 또는 0)를 얻을 수 있는 선택을 할 수 있다. 즉, 32개의 링 오실레이터 셀에서 하나를 선택하는 경우이므로 2^5 = 32가 되어 m=5가 되고 총 20bit를 구성할 수 있다. 이러한 링 오실레이터 셀의 선택 값을 이용할 경우, 최종 결정되는 비밀키 정보(1 또는 0)를 '응답(response)'으로 정의할 수 있으며, 하나의 응답(response)을 얻기 위해 입력되는 링 오실레이터 셀의 선택정보를 '시도(challenge)'으로 정의할 수 있다.

[0055] 일반적으로 PUF에서 하나의 시도(challenge)에 대한 하나의 응답(response)을 '시도-응답 쌍(challenge-response pair)'이라고 정의하는데, 얼마나 다른 경우의 시도-응답 쌍을 만들어 낼 수 있는지가 PUF의 성능을 나타낼 수 있다. 즉, 다양한 수의 시도-응답 쌍이 존재해야 이를 이용한 암호 key 생성 및 ID 생성 시 유일성(uniqueness)을 확보할 수 있다.

[0056] 본 개시의 일 실시예에 따른 비밀 정보 생성 장치에 따르면, 두 개의 PUF 정보 생성부를 통해 출력되는 클럭신호를 서로 교차하여 타겟 신호와 레퍼런스 신호로서 사용하여, 두 개의 위상신호를 기반으로 하는 카운트 값을 생성하고, 또한, PUF 정보 생성부에 구비된 MUX를 통해 다수의 레퍼런스 신호와 다수개의 타겟신호를 조합할 수 있다.

[0057] 이와 같이, 본 발명의 일 실시예에 따른 비밀 정보 생성 장치를 통해 종래에 비하여 상대적으로 많은 수의 시도-응답 쌍을 생성할 수 있다. 예컨대, 두개의 PUF 정보 생성부에 각각 32개의 링 오실레이터 셀이 구비될 경우,

약 1백만개의 시도-응답 쌍을 구성할 수 있다.

[0058] 본 개시의 예시적인 방법들은 설명의 명확성을 위해서 동작의 시리즈로 표현되어 있지만, 이는 단계가 수행되는 순서를 제한하기 위한 것은 아니며, 필요한 경우에는 각각의 단계가 동시에 또는 상이한 순서로 수행될 수도 있다. 본 개시에 따른 방법을 구현하기 위해서, 예시하는 단계에 추가적으로 다른 단계를 포함하거나, 일부의 단계를 제외하고 나머지 단계를 포함하거나, 또는 일부의 단계를 제외하고 추가적인 다른 단계를 포함할 수도 있다.

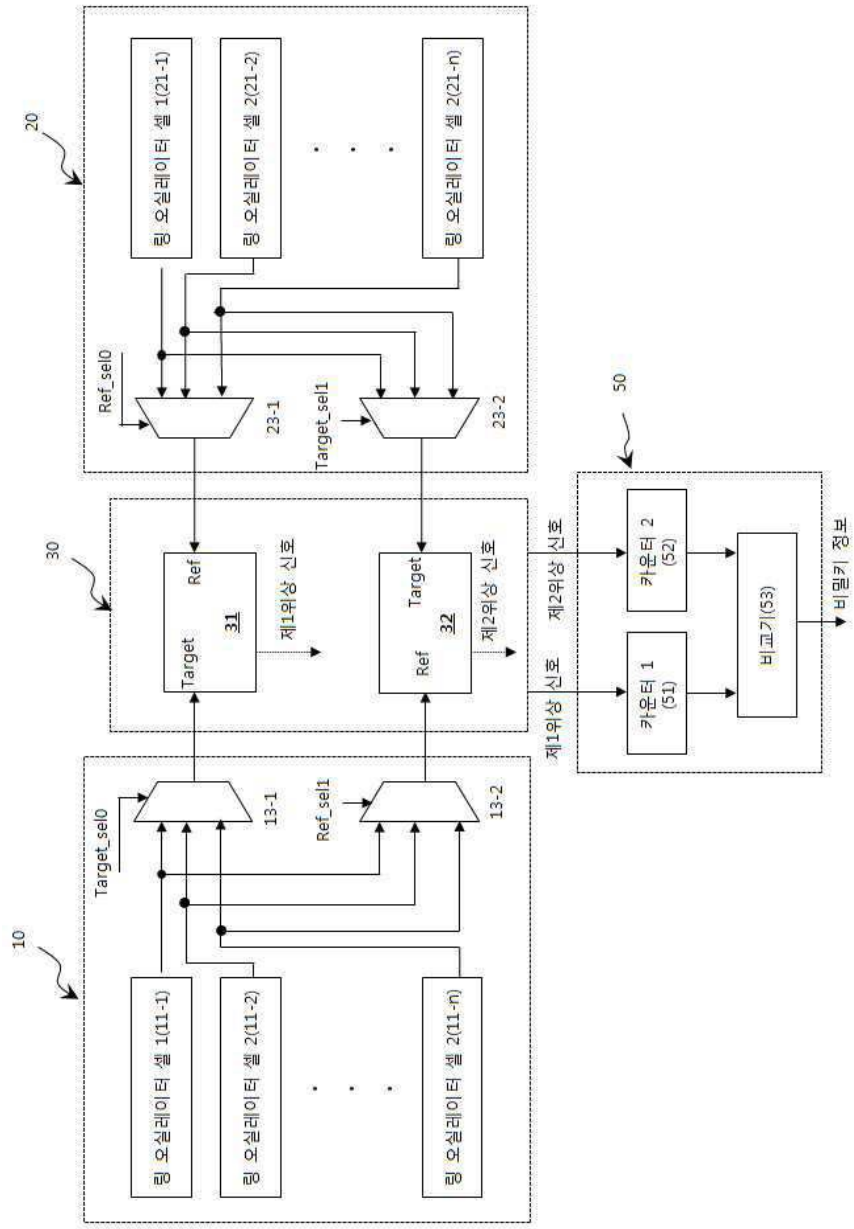
[0059] 본 개시의 다양한 실시 예는 모든 가능한 조합을 나열한 것이 아니고 본 개시의 대표적인 양상을 설명하기 위한 것이며, 다양한 실시 예에서 설명하는 사항들은 독립적으로 적용되거나 또는 둘 이상의 조합으로 적용될 수도 있다.

[0060] 또한, 본 개시의 다양한 실시 예는 하드웨어, 펌웨어(firmware), 소프트웨어, 또는 그들의 결합 등에 의해 구현될 수 있다. 하드웨어에 의한 구현의 경우, 하나 또는 그 이상의 ASICs(Application Specific Integrated Circuits), DSPs(Digital Signal Processors), DSPDs(Digital Signal Processing Devices), PLDs(Programmable Logic Devices), FPGAs(Field Programmable Gate Arrays), 범용 프로세서(general processor), 컨트롤러, 마이크로 컨트롤러, 마이크로 프로세서 등에 의해 구현될 수 있다.

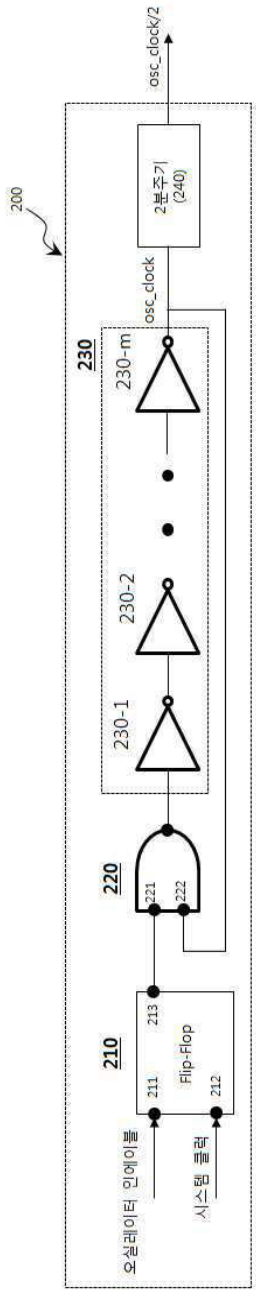
[0061] 본 개시의 범위는 다양한 실시 예의 방법에 따른 동작이 장치 또는 컴퓨터 상에서 실행되도록 하는 소프트웨어 또는 머신-실행가능한 명령들(예를 들어, 운영체제, 애플리케이션, 펌웨어(firmware), 프로그램 등), 및 이러한 소프트웨어 또는 명령 등이 저장되어 장치 또는 컴퓨터 상에서 실행 가능한 비-일시적 컴퓨터-판독가능 매체(non-transitory computer-readable medium)를 포함한다.

도면

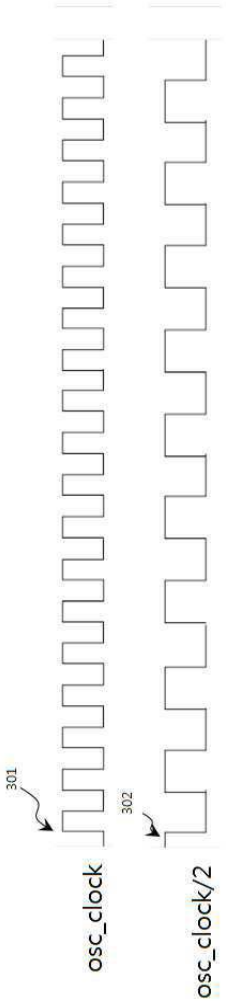
도면1


10
20
30
50
링 오실레이터 셀 1(11-1)
링 오실레이터 셀 2(11-2)
링 오실레이터 셀 2(11-n)
링 오실레이터 셀 1(21-1)
링 오실레이터 셀 2(21-2)
링 오실레이터 셀 2(21-n)
Target_sel0
Ref_sel1
13-1
13-2
Ref_sel0
Target_sel1
23-1
23-2
Target
Ref
31
Ref
Target
32
제1위상 신호
제2위상 신호
제1위상 신호
제2위상 신호
카운터 1 (51)
카운터 2 (52)
비교기(53)
비밀키 정보

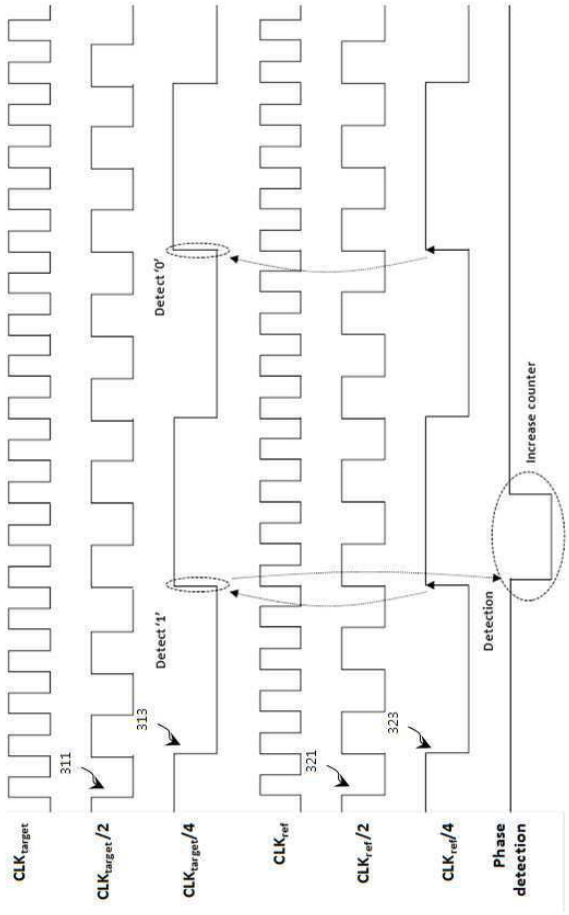
도면2


200
osc_clock/2
2분주기
(240)
osc_clock
230
230-m
230-2
230-1
220
221
222
210
213
Flip-Flop
211
212
오실레이터 인에이블
시스템 클럭

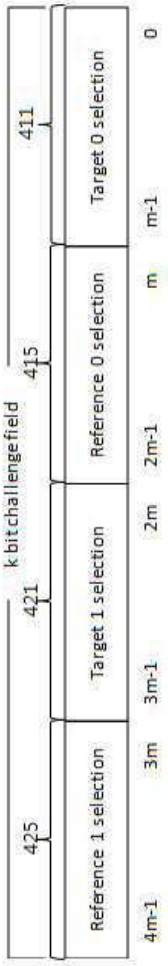
도면3a



도면3b


CLK target
CLK target /2
CLK target /4
CLK ref
CLK ref /2
CLK ref /4
Phase detection
311
313
321
323
Detect '0'
Detect '1'
Detection
Increase counter

도면4


k bit challenge field
425
421
415
411
Reference 1 selection
Target 1 selection
Reference 0 selection
Target 0 selection
4m-1
3m
3m-1
2m
2m-1
m
m-1
0