(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년10월01일
(11) 등록번호 10-1987141
(24) 등록일자 2019년06월03일

(51) 국제특허분류(Int. Cl.)
G06F 7/58 (2006.01)
(21) 출원번호 10-2013-0022851
(22) 출원일자 2013년03월04일
심사청구일자 2018년02월06일
(65) 공개번호 10-2014-0110142
(43) 공개일자 2014년09월17일
(56) 선행기술조사문헌
KR101127961 B1
JP2007207054 A
KR1020130003709 A
KR1020120101837 A

(73) 특허권자
삼성전자주식회사
경기도 수원시 영통구 삼성로 129 (매탄동)
(72) 발명자
바실조프이호르
경기 수원시 영통구 영통로 460, 306동 1801호 (영통동, 청명마을3단지아파트)
카르핀스키보단
경기도 수원시 영통구 매영로310번길 12 325동 1702호 (영통동,신나무실5단지아파트)
(뒷면에 계속)
(74) 대리인
특허법인 고려

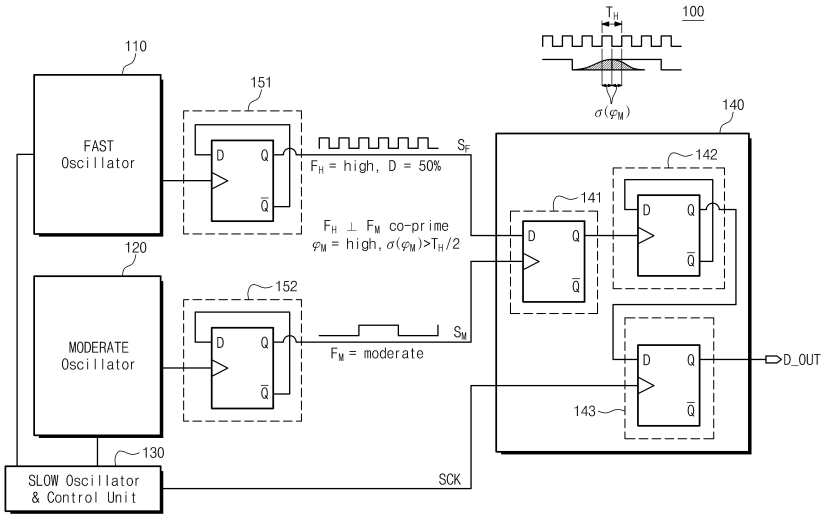
전체 청구항 수 : 총 10 항 심사관 : 지정훈

(54) 발명의 명칭 **난수 발생기**

(57) 요 약

본 발명에 따른 난수 발생기는, 제 1 주파수를 갖는 제 1 발진 신호를 출력하는 제 1 발진기; 상기 제 1 주파수와 다른 제 2 주파수를 갖는 제 2 발진 신호를 출력하는 제 2 발진기; 상기 제 1 발진 신호 및 상기 제 2 발진 신호를 입력 받고, 상기 입력된 제 1 및 제 2 발진 신호들을 조합하여 적어도 하나의 엔트로피 소스를 발생하고, 상기 발생된 엔트로피 소스에 대응하는 비트를 제 3 발진 신호를 이용하여 샘플링하는 샘플링부; 및 상기 제 1 및 제 2 발진기들을 제어하고, 상기 제 3 발진 신호를 발생하는 제 3 발진기 및 제어부를 포함하고, 상기 제 3 발진 신호의 주파수는 상기 제 1 및 제 2 주파수들보다 낮다.

대 표 도



(72) 발명자

이헌수

경기도 화성시 동탄반석로 277 122동 1402호 (석우동,예당마을우미린제일풍경채아파트)

최윤혁

경상남도 창원시 성산구 반송로 177 204동 1005호 (반림동,현대2차아파트)

명 세 서

청구범위

청구항 1

제 1 주파수를 갖는 제 1 발진 신호를 출력하는 제 1 발진기;

상기 제 1 주파수와 다른 제 2 주파수를 갖는 제 2 발진 신호를 출력하는 제 2 발진기;

상기 제 1 발진 신호 및 상기 제 2 발진 신호를 입력 받고, 상기 입력된 제 1 및 제 2 발진 신호들을 조합하여 적어도 하나의 엔트로피 소스를 발생하고, 상기 발생된 엔트로피 소스에 대응하는 비트를 제 3 발진 신호를 이용하여 샘플링하는 샘플링부; 및

상기 제 1 및 제 2 발진기들을 제어하고, 상기 제 3 발진 신호를 발생하는 제 3 발진기 및 제어부를 포함하고,

상기 제 3 발진 신호의 주파수는 상기 제 1 및 제 2 주파수들보다 낮은 난수 발생기.

청구항 2

제 1 항에 있어서,

상기 제 1 발진 신호 및 상기 제 2 발진 신호는 코-프라임(co-prime)하는 난수 발생기.

청구항 3

제 1 항에 있어서,

상기 제 1 주파수가 상기 제 2 주파수보다 높게 설정된 난수 발생기.

청구항 4

제 3 항에 있어서,

상기 제 2 발진 신호는 지터를 갖는 중속 신호이고,

상기 중속 신호의 위상에 대한 표준 편차는 상기 제 1 발진 신호의 주기의 절반보다 큰 난수 발생기.

청구항 5

제 3 항에 있어서,

상기 제 2 발진기는 준안정성 모드에서 노이즈 소스를 발생하고, 상기 발생된 노이즈 소스를 증폭하는 복수의 발진부들을 포함하고, 발진 모드에서 상기 복수의 발진부들을 하나의 링 오실레이터로 구성되는 난수 발생기.

청구항 6

제 1 항에 있어서,

상기 제 1 주파수는 상기 제 2 주파수보다 낮은 난수 발생기.

청구항 7

제 1 항에 있어서,

상기 샘플링부는,

상기 엔트로피 소스를 발생하기 위하여 상기 제 2 발진 신호에 응답하여 상기 제 1 발진 신호를 샘플링하는 제 1 샘플링부;

상기 발생된 엔트로피를 축적하기 위하여 상기 제 1 샘플링부의 출력을 카운팅하는 2 모드 카운터; 및

상기 비트를 출력하기 위하여 상기 2 모드 카운터의 출력을 상기 제 3 발진 신호에 응답하여 샘플링하는 제 2

샘플링부를 포함하는 난수 발생기.

청구항 8

제 1 항에 있어서,

상기 샘플링부는,

상기 제 1 발진 신호를 카운팅하는 2 모드 카운터;

상기 제 2 발진 신호 및 상기 제 3 발진 신호를 앤드 연산하는 앤드 논리 회로; 및

상기 2 모드 카운터의 출력을 상기 앤드 논리 회로의 출력에 응답하여 샘플링하는 마스터 샘플링부를 포함하는 난수 발생기.

청구항 9

제 1 항에 있어서,

상기 제 1 발진 신호의 듀티 싸이클을 보정하기 위하여 상기 제 1 발진기의 출력단에 연결된 듀티 싸이클 교정기를 더 포함하는 난수 발생기.

청구항 10

제 1 주파수를 갖는 제 1 발진 신호를 발생하는 제 1 발진기;

상기 제 1 주파수보다 느린 제 2 주파수를 갖는 제 2 발진 신호를 발생하는 적어도 하나의 제 2 발진기;

상기 제 1 및 제 2 발진 신호들을 이용하여 적어도 2개의 엔트로피 소스들을 발생하기 위하여 제 1 샘플링들을 수행하고, 상기 제 1 샘플링들의 결과값들을 논리 연산하고, 상기 논리 연산된 결과값을 제 3 발진 신호에 응답하여 제 2 샘플링하는 샘플링부; 및

상기 제 1 및 제 2 발진기들을 제어하고, 상기 제 3 발진 신호를 발생하는 제 3 발진기 및 제어부를 포함하는 난수 발생기.

발명의 설명

기 술 분 야

[0001] 본 발명은 난수 발생기에 관한 것이다.

배 경 기 술

[0002] 정보 통신 기술의 발전에 따라서, 정보의 암호화 및 복호화 기술은 해당 정보의 보안 유지를 위하여 매우 중요시되고 있다. 난수(random number)는 보안 시스템(security system)의 비밀키(secret key)를 비롯한 여러 곳에서 사용된다. 따라서, 보안이 중요시되는 시스템은 난수 발생기(random number generator)가 구비되며, 난수 발생기는 예측 불가능한 값을 갖는 난수를 발생시켜야만 한다. 보안이 중요시되는 시스템에 있어서, 난수는 주기성과 규칙성을 가져서는 안 된다. 즉, 보안 시스템에서는 예측이 불가능하고 어떠한 주기성도 갖지 않는 완전한 난수를 발생시킬 필요가 있는 것이다.

[0003] 참 난수(true random number, 이하 'TRN')는 물리적 노이즈 소스(physical noise source)으로부터 발생되며, 예측 불가능하고 어떠한 주기성도 갖지 않는다. 이러한 참 난수를 발생시키기 위하여, 기존의 난수 발생 장치는 노이즈 소스로써 열적 노이즈(thermal noise) 또는 샷 노이즈(shot noise)를 이용하였다. 또는 링 오실레이터를 이용하여 불규칙한 주기를 갖는 클록 신호를 발생시켜 이용하였다. 준안정성(meta-stability)은 좋은 확률적인 특성(stochastic properties)을 보이는 것으로 알려져 있기 때문에, 진성난수 발생기(TRNG; true random number generator)에 널리 사용되고 있다. 종래에는 이러한 준안정성 상태(meta-stability state)를 이용하기 위하여, 래치 또는 플립 플롭을 주로 사용하였다.

발명의 내용

해결하려는 과제

[0004] 본 발명의 목적은 효율적(면적/전력소모)이면서 고속으로 등가 분포의 난수를 발생하는 난수 발생기를 제공하는 데 있다.

과제의 해결 수단

[0005] 본 발명의 실시 예에 따른 난수 발생기는, 제 1 주파수를 갖는 제 1 발진 신호를 출력하는 제 1 발진기; 상기 제 1 주파수와 다른 제 2 주파수를 갖는 제 2 발진 신호를 출력하는 제 2 발진기; 상기 제 1 발진 신호 및 상기 제 2 발진 신호를 입력 받고, 상기 입력된 제 1 및 제 2 발진 신호들을 조합하여 적어도 하나의 엔트로피 소스를 발생하고, 상기 발생된 엔트로피 소스에 대응하는 비트를 제 3 발진 신호를 이용하여 샘플링하는 샘플링부; 및 상기 제 1 및 제 2 발진기들을 제어하고, 상기 제 3 발진 신호를 발생하는 제 3 발진기 및 제어부를 포함하고, 상기 제 3 발진 신호의 주파수는 상기 제 1 및 제 2 주파수들보다 낮다.

[0006] 실시 예에 있어서, 상기 제 1 발진 신호 및 상기 제 2 발진 신호는 코-프라임(co-prime)이다.

[0007] 실시 예에 있어서, 상기 제 1 주파수가 상기 제 2 주파수보다 높다.

[0008] 실시 예에 있어서, 상기 제 1 발진 신호는 등가 분포의 고속 신호이다.

[0009] 실시 예에 있어서, 상기 고속 신호는 50%의 듀티 싸이클을 갖는다.

[0010] 실시 예에 있어서, 상기 제 2 발진 신호는 높은 지터를 갖는 중속 신호이다.

[0011] 실시 예에 있어서, 상기 중속 신호의 위상에 대한 표준 편차는 상기 제 1 발진 신호의 주기의 절반보다 크다.

[0012] 실시 예에 있어서, 상기 제 1 발진기는, 초기 신호 및 상기 제 1 발진 신호를 낸드 연산하는 낸드 논리 회로; 상기 낸드 논리 회로의 출력을 반전하는 제 1 인버터; 및 상기 제 1 인버터의 출력을 반전시킴으로써 상기 제 1 발진 신호를 출력하는 제 2 인버터를 포함한다.

[0013] 실시 예에 있어서, 상기 제 2 발진기는 준안정성 모드에서 노이즈 소스를 발생하고, 상기 발생된 노이즈 소스를 증폭하는 복수의 발진부들을 포함하고, 상기 발진 모드에서 상기 복수의 발진부들을 하나의 링 오실레이터로 구성된다.

[0014] 실시 예에 있어서, 상기 제 1 주파수는 상기 제 2 주파수보다 낮다.

[0015] 실시 예에 있어서, 상기 샘플링부는, 상기 엔트로피 소스를 발생하기 위하여 상기 제 2 발진 신호에 응답하여 상기 제 1 발진 신호를 샘플링하는 제 1 샘플링부; 상기 발생된 엔트로피를 축적하기 위하여 상기 제 1 샘플링부의 출력을 카운팅하는 2 모드 카운터; 및 상기 비트를 출력하기 위하여 상기 2 모드 카운터의 출력을 상기 제 3 발진 신호에 응답하여 샘플링하는 제 2 샘플링부를 포함한다.

[0016] 실시 예에 있어서, 상기 샘플링부는, 상기 제 1 발진 신호를 카운팅하는 2 모드 카운터; 상기 제 2 발진 신호 및 상기 제 3 발진 신호를 앤드 연산하는 앤드 논리 회로; 및 상기 2 모드 카운터의 출력을 상기 앤드 논리 회로의 출력에 응답하여 샘플링하는 마스터 샘플링부를 포함한다.

[0017] 실시 예에 있어서, 상기 제 1 발진 신호의 듀티 싸이클을 보정하기 위하여 상기 제 1 발진기의 출력단에 연결된 듀티 싸이클 교정기를 더 포함한다.

[0018] 본 발명의 다른 실시 예에 따른 난수 발생기는, 제 1 주파수를 갖는 제 1 발진 신호를 발생하는 제 1 발진기; 상기 제 1 주파수보다 느린 제 2 주파수를 갖는 제 2 발진 신호를 발생하는 적어도 하나의 제 2 발진기; 상기 제 1 및 제 2 발진 신호들을 이용하여 적어도 2개의 엔트로피 소스들을 발생하기 위하여 제 1 샘플링들을 수행하고, 상기 제 1 샘플링들의 결과값들을 논리 연산하고, 상기 논리 연산된 결과값을 제 3 발진 신호에 응답하여 제 2 샘플링하는 샘플링부; 및 상기 제 1 및 제 2 발진기들을 제어하고, 상기 제 3 발진 신호를 발생하는 제 3 발진기 및 제어부를 포함한다.

[0019] 실시 예에 있어서, 상기 논리 연산은 배타적 논리합이다.

발명의 효과

[0020] 상술한 바와 같이 본 발명에 따른 난수 발생기는 고속의 발진 신호와 중속의 발진 신호를 조합하여 엔트로피 소스를 발생함으로써, 등가 분포를 가지면서도 효율적으로 난수를 발생시킨다.

도면의 간단한 설명

[0021] 도 1은 본 발명의 실시 예에 따른 난수 발생기에 대한 제 1 실시 예를 보여주는 도면이다.

도 2는 도 1에 도시된 제 1 발진기에 대한 실시 예를 보여주는 도면이다.

도 3은 도 1에 도시된 제 2 발진기에 대한 실시 예를 보여주는 도면이다.

도 4는 본 발명의 실시 예에 따른 난수 발생기에 대한 제 2 실시 예를 보여주는 도면이다.

도 5는 본 발명의 실시 예에 따른 난수 발생기에 대한 제 3 실시 예를 보여주는 도면이다.

도 6은 본 발명의 실시 예에 따른 난수 발생기에 대한 제 4 실시 예를 보여주는 도면이다.

도 7은 본 발명의 실시 예에 따른 난수 발생기에 대한 제 5 실시 예를 보여주는 도면이다.

도 8은 본 발명의 실시 예에 따른 난수 발생기에 대한 제 6 실시 예를 보여주는 도면이다.

도 9는 본 발명의 실시 예에 따른 난수 발생기를 갖는 암호 프로세서를 포함하는 보안 시스템을 예시적으로 보여주는 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0022] 이하, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 본 발명의 기술적 사상을 용이하게 실시할 수 있도록 본 발명의 실시 예를 첨부된 도면을 참조하여 설명할 것이다.

[0023] 본 발명은 등가 분포로 고속(fast)의 발진 신호와 높은 지터를 갖는 중속(moderate)의 발진 신호를 이용하여 엔트로피 소스를 발생함으로써, 효율적(면적/전력소모)이면서 고속으로 등가 분포의 난수를 발생하는 난수 발생기를 제공할 것이다.

[0024] 도 1은 본 발명의 실시 예에 따른 난수 발생기에 대한 제 1 실시 예를 보여주는 도면이다. 도 1을 참조하면, 난수 발생기는 제 1 발진기(110), 제 2 발진기(120), 제 3 발진기 및 제어 유닛(130), 샘플링부(140), 및 제 1 및 제 2 듀티 싸이클 교정기들(151, 152)을 포함한다.

[0025] 제 1 발진기(110, 고속 발진기)는 등가 분포된 제 1 발진 신호(S_F, 혹은, '고속 신호')를 출력한다. 여기서 제 1 발진 신호(S_F)는 샘플링을 위한 원스 앤 제로스 순환 패턴(cyclic pattern of ones and zeros)일 수 있다. 등가 분포된 난수를 얻기 위해서 샘플링된 패턴에서 원스(ones)의 확률은 제로스(zeros)의 확률과 동일 할 것이다. 예를 들어, Pr(1) = Pr(0) = 0.5 이다. Pr(1)는 발생된 신호의 듀티 사이클(duty cycle)에 직접적으로 비례한다. 예를 들어, $Pr(1) \propto D$ 이다. 여기서 D는 듀티 싸이클이다. 따라서 듀티 사이클 D = 50% 될 것이다.

[0026] 제 1 발진 신호(S_F)의 주파수(F_H)는 난수 발생의 성능에 있어서 최대 제한이고, 가능하면 높게 설정될 것이다.

[0027] 제 2 발진기(120, 중속 발진기)는 엔트로피의 메인 소스로써 제 2 발진 신호(S_M, 혹은 '중속 신호')를 출력할 것이다. 출력되는 제 2 발진 신호(S_M)의 위상 표준편차는, $\sigma(\varphi_M) > \frac{T_H}{2}$ 만족시킬 것이다. 여기서 T_H는 제 1 발진 신호(S_F)의 주기의 절반이다. 제 2 발진기(120)의 주파수(F_M)는 충분하게 엔트로피를 축적하도록 선택될 것이다.

[0028] 또한, 제 1 발진기(110)의 주파수(F_H)와 제 2 발진기(120)의 주파수(F_M)는 발진기들(110, 120)의 "잠금"(locking)의 기회를 최소화시키기 위하여 코-프라임($F_H \perp F_M$, 서로소)으로 선택될 것이다. 제 2 발진기(120)의 듀티 사이클(D)의 값은 임의의 값이다.

[0029] 제 3 발진기(저속 발진기) 및 제어 유닛(130)은, 제 1 및 제 2 발진기들(110, 120)을 제어하고, 샘플링부(140)로 샘플링 클록(SCK, 혹은 '제 3 발진 신호'; '저속 신호')을 출력시킨다. 여기서 샘플링 클록(SCK)의 주파수는 제 1 발진기(110)의 주파수(F_H) 및 제 2 발진기(120)의 주파수(F_M) 보다 낮을 것이다. 다른 말로, 제 3 발진기 및 제어 유닛(130)은, 서로 다른 사용 케이스 시나리오(높은 엔트로피, 고성능, 저전력 등)을 위하여 난수 발생기(100)의 높은 유연성을 제공하도록, 목표 주파수를 갖는 중속 발진기(120)에 의해 빠른 발진기(110)의 샘플링을 동기화하도록 샘플링 클록(SCK)을 제공한다.

[0030] 제 3 발진기 및 제어 유닛(130)은 제 1 발진기(110) 및 제 2 발진기 (120)의 작동을 제어한다. 여기서 제 1 발진기(110)는 모든 임의의 비트 발생을 위하여 소정의 값으로 재설정되도록 구현될 수 있다. 이를 위해, 제 3 발진기 및 제어 유닛(130)은, 활성 모드/비활성 모드 사이에 정기적으로 변경하는 활성화 신호(EN)를 발생할 수 있다.

[0031] 샘플링부(140)는 제 1 발진 신호(S_F), 제 2 발진 신호(S_M) 및 샘플링 클록(SCK)을 입력 받고, 제 2 발진기(120)로부터 출력되는 엔트로피 소스에 대응하는 랜덤 비트를 출력단(D_OUT)을 통하여 출력한다. 즉, 샘플링부(140)는 3개의 발진기들(고속 발진기(110), 중속 발진기(120), 저속 발진기(130))에 의해 발생된 랜덤 비트로 출력한다. 샘플링부(140)는 제 1 샘플링부(141, 혹은 '프리 샘플링부'), 2 모드 카운터(142), 및 제 2 샘플링부(143, 혹은 '마스터 샘플링부'; '메인 샘플링부')를 포함한다.

[0032] 제 1 샘플링부(141)는 제 2 발진 신호(S_M)에 응답하여 제 1 발진 신호(S_F)를 샘플링함으로써, 제 1 발진기(110)와 제 2 발진기(120) 사이의 위상 차이($\triangle\phi = \phi_H - \phi_M$)에 따른 엔트로피를 출력한다. 만일, 위상 차이($\triangle\phi$)가 크다면(예를 들어, $\sigma(\phi_M) > T_H/2$), 제 1 발진기(110, 고속 발진기)의 주기 관점에서, 샘플링 펄스(예를 들어, 제 2 발진 신호(S_M))의 위치에 상관없이 충분한 엔트로피가 샘플될 수 있다.

[0033] 2 모드 카운터(142)는, 제 1 샘플링부(141)의 출력이 변경될 때마다, 엔트로피를 축적하도록 카운팅할 것이다. 따라서, 엔트로피는 초기값으로부터 보다 압축될 것이다.

[0034] 제 2 샘플링부(143)는 샘플 클록(SCK, 혹은 '제 3 발진 신호' ; '저속 신호')에 응답하여 2 모드 카운터(142)의 출력값을 샘플링할 것이다.

[0035] 제 1 듀티 싸이클 교정기(151)는, 제 1 발진기(110)로 출력된 제 1 발진 신호(S_F)의 듀티 싸이클을 교정한다. 제 1 듀티 싸이클 교정기(151)는 도 1에 도시된 바와 같이 D-Q 플립플롭으로 구현될 수 있다.

[0036] 제 2 듀티 싸이클 교정기(152)는, 제 2 발진기(120)로부터 출력된 제 2 발진 신호(S_M)의 듀티 싸이클을 교정한다. 제 2 듀티 싸이클 교정기(152)는 도 1에 도시된 바와 같이 D-Q 플립플롭으로 구현될 수 있다.

[0037] 한편, 제 1 및 제 2 듀티 싸이클 교정기(151, 152) 중 적어도 하나는 생략될 수도 있다.

[0038] 본 발명의 실시 예에 따른 난수 발생기(100)는 제 1 발진기(110)로부터 출력되는 등가 분포의 고속 신호(S_F)와 제 2 발진기(120)로부터 출력되는 높은 지터의 중속 신호(S_M)을 조합하여 엔트로피 소스를 발생함으로써, 등가 분포이면서 높은 엔트로피를 갖는 난수를 발생할 수 있다.

[0039] 도 2는 도 1에 도시된 제 1 발진기(110)에 대한 실시 예를 보여주는 도면이다. 도 2를 참조하면, 제 1 발진기(110)는 낸드 논리회로(111), 제 1 인버터(112) 및 제 2 인버터(123)를 포함한다. 낸드 논리회로(111)는 입력 신호와 피드백된 출력 신호를 낸드 연산을 수행한다. 제 1 인버터(112)는 낸드 논리회로(111)의 출력을 반전시키고, 제 2 인버터(113)는 제 1 인버터(112)의 출력을 반전시킨다. 이로서 링 오실레이터를 구성함으로써 제 1 발진 신호(S_F)가 발생될 것이다. 한편, 본 발명의 제 1 발진기(110)의 구조가 도 2에 도시된 구성에 제한되지 않을 것이다. 본 발명에 따른 제 1 발진기(110)은 제 1 발진 신호(S_F)를 발생하는 링 오실레이터로 다양하게 구현될 수 있다.

[0040] 한편, 엔트로피의 메인 소스를 발생하는 본 발명의 실시 예에 따른 제 2 발진기(120)는 메타 오실레이터(meta-oscillator)로 구현 가능하다.

[0041] 도 3은 도 1에 도시된 제 2 발진기(120)에 대한 실시 예를 보여주는 도면이다. 도 3을 참조하면, 제 2 발진기(120)는 복수의 발진 유닛들(121, 122, ..., 12n, n은 2 이상의 정수)을 포함한다. 실시 예에 있어서, 제 2 발진기(120)는 메타-오실레이터일 수 있다. 발진 유닛들(121, 122, ..., 12n) 각각은 직렬 연결된 스위칭 장치 및 복수의 인버터들을 포함한다.

[0042] 제 2 발진기(120)는 모드 신호(mode)에 따라 준안정성 모드(meta-stability mode) 및 발진 모드(oscillation mode) 중 어느 하나로 동작할 것이다.

[0043] 첫째로, 준안정성 모드 동작은 다음과 같다. 준안정성 모드에서, 인버터들(INV11, INV21, ..., INVn1)은 스위칭 장치들(MUX1, MUX2, ..., MUXn)에 의해 준안정성 레벨로 수렴하도록 고정될 것이다. 이에 통계적으로 아날로그

신호들을 제공하는 n 개의 엔트로피의 소스들이 발생된다. 발생된 엔트로피 소스들은 직렬 연결된 인버터들로 구성된 증폭 체인에 연결될 것이다. 예를 들어, INV12에서 INV1k는 제 1 증폭 체인을 형성하고, INV22에서 INV2k 는 제 2 증폭 체인을 형성한다. 증폭 체인에 사용되는 인버터들 개수(k)는 목표로 하는 기술에서 하나의 인버터의 이득 값에 의존하고, 통계적인 아날로그 신호의 충분한 증폭을 제공하도록 선택될 수 있다.

[0044] 엔트로피 소스들의 개수(n)는 목표로 하는 기술 공정의 변화 및 불일치 특성에 의존하고, 엔트로피 소스의 통계적인 아날로그 신호의 평균 값이 대응하는 증폭 체인으로부터 제 1 인버터의 문턱 레벨에 일치한다는 충분한 확률을 제공하도록 계산될 것이다. 여기서 증폭 체인에서 제 1 인버터 및 다음 인버터 사이의 문턱 레벨들의 불일치는 무시할 것이다. 하지만, 다른 기술에는 이러한 불일치를 무시하지 않고 반영될 수도 있다.

[0045] 둘째로, 발진 동작은 다음과 같다. 스위칭 장치들(MUX1, MUX2, ..., MUXn)은 링 발진기를 형성하도록 모드 신호(mode)에 응답하여 변환될 것이다. 도 3에 도시된 바와 같이, 링 발진기는 MUX1 → INV11 → INV12 → ... → INV1k → MUX2 → INV21 → INV22 ... → MUXn → INVn1 → MUX1 로 구성될 것이다. 대개, 링 발진기를 형성하기 위하여 인버터들의 개수는 홀수이다. 변환 후에, 제 2 발진기(120)는 결정된 중속 주파수(F_M) 및 임의 위상(ϕ_M)을 갖는 발진기 신호를 발생할 것이다.

[0046] 여기서 중속 주파수(F_M)의 값은 CMOS 인버터 특성들에 의해 정의되고, 제조 기술의 특성에 의존할 것이다. 여기서 위상(ϕ_M)의 값은 발진 모드 전에 발진기를 형성하는 대응하는 인버터들로부터 발진 신호들의 모멘텀(momentum) 값들로부터 결정될 것이다. 발진 신호들의 이러한 모멘텀 값들은 통계적인 아날로그 신호들로부터 형성되고, 그것들은 임의성을 상속하고 엔트로피를 포함할 것이다. 따라서, 초기 위상 값(ϕ_M)은 임의적이다. 만일, 초기 엔트로피가 충분히 크지 않으면, 난수 발생기(100, 도 1 참조)는 지터로써 추가적인 엔트로피를 축적하는 발진 모드에서 계속적으로 동작할 것이다.

[0047] 한편, 도 3에 도시된 제 2 발진기(120)는 실시 예에 불과하다. 본 발명에 따른 제 2 발진기(120)는 다양한 방법 및 구성으로 메타-오실레이터를 구현할 수 있다.

[0048] 한편, 도 1에 도시된 난수 발생기는 샘플링 클록(SCK)에 응답하여 엔트로피 소스에 대응하는 비트를 샘플링함으로써 랜덤 비트를 발생하였다. 하지만, 본 발명이 반드시 샘플링 클록(SCK)에 따라 샘플링할 필요는 없다. 본 발명의 실시 예에 따른 난수 발생기는 샘플링 클록(SCK)과 메인 엔트로피 소스로 사용되는 제 2 발진 신호(S_M)를 조합한 신호에 따라 샘플링함으로써, 특정한 시간에 샘플링되도록 하는 엔트로피를 추가할 수 있다.

[0049] 도 4는 본 발명의 실시 예에 따른 난수 발생기에 대한 제 2 실시 예를 보여주는 도면이다. 도 4를 참조하면, 난수 발생기(200)는 제 1 발진기(210), 제 2 발진기(220), 제 3 발진기 및 제어 유닛(230), 샘플링부(240), 및 제 1 및 제 2 듀티 싸이클 교정기들(251, 252)을 포함한다.

[0050] 제 1 발진기(210)는, 도 2에 도시된 제 1 발진기(110)과 비교하여 제 1 발진 신호(S_F)의 주파수를 변량 할 수 있는 구조이다. 제 2 발진기(220)의 초기 단계 및 주파수와 일치에 적합할 적절한 값을 선택하도록 제 1 발진기(210)의 주파수를 조절함으로써, 더 많은 엔트로피가 얻어질 수 있다.

[0051] 샘플링부(240)는 카운터(241), 앤드 논리 회로(242), 및 마스터 샘플링부(243)를 포함한다. 카운터(241)는 고속 발진기의 주기들의 개수의 나머지 값을 축적할 것이다. 마스터 샘플링부(243)는 샘플링 클록(SCK)의 구성에 따라 값을 샘플링 한다. 앤드 논리 회로(242)는 시간의 특정한 모멘트에서 샘플링하도록 하기 위한 엔트로피를 제공한다.

[0052] 실시 예에 있어서, 제 2 발진기(220, 중속 발진기)의 듀티 싸이클은 가능한 작을 것이다.

[0053] 본 발명의 실시 예에 따른 난수 발생기(200)는 샘플링 클록(SCK)과 제 2 발진 신호(S_M)을 이용하여 랜덤 비트를 샘플링함으로써, 샘플링하기 위한 클록의 엔트로피를 발생할 수 있다.

[0054] 한편, 도 1의 샘플링부(140)에서는 중속 신호인 제 2 발진 신호(S_M)에 응답하여 고속 신호인 제 1 발진 신호(S_F)를 샘플링하였다. 하지만, 본 발명은 여기에 제한되지 않을 것이다. 본 발명의 샘플링부는 1 발진 신호(S_F)에 응답하여 중속 신호인 제 2 발진 신호(S_M)를 샘플링할 수도 있다. 즉, 제 1 발진기(110) 및 제 2 발진기(120)의 기능적인 위치가 서로 바뀔 수 있다.

[0055] 도 5는 본 발명의 실시 예에 따른 난수 발생기에 대한 제 3 실시 예를 보여주는 도면이다. 도 5를 참조하면, 난

수 발생기(300)는 제 1 발진기(310), 제 2 발진기(320), 제 3 발진기 및 제어 유닛(330), 샘플링부(340), 제 1 및 제 2 듀티 싸이클 교정기들(351, 352)을 포함한다. 여기서 제 1 발진기(310)는 도 3에 도시된 제 2 발진기(120)와 동일한 구성이고, 제 2 발진기(320)는 도 2에 도시된 제 1 발진기(110)와 동일한 구성일 것이다. 즉, 제 1 발진기(310)는 중속 발진기이고, 제 2 발진기(320)는 고속 발진기이다.

[0056] 제 2 발진기(320)의 모든 라이징에 따라 제 1 발진기(310)의 신호가 샘플될 것이다. 즉, 제 2 발진기(320)의 듀티 싸이클은 임의로 될 수 있다. 그러나 제 1 발진기(310)의 듀티 싸이클은 D = 50 %이어야 한다.

[0057] 본 발명의 실시 예에 따른 난수 발생기는 고속 신호(S_F)에 응답하여 중속 신호(S_M)를 샘플링할 수 있다.

[0058] 도 1 내지 도 5에서는 고속 신호(S_F)와 중속 신호(S_M)를 이용하여 하나의 엔트로피 소스에 대응하는 랜덤 비트를 발생하였다. 하지만 본 발명이 여기에 제한되지 않을 것이다. 본 발명은 고속 신호(S_F)와 중속 신호(S_M)를 이용하여 복수의 엔트로피 소스들을 발생하고, 발생된 복수의 엔트로피 소스들 중에 어느 하나를 선택할 수도 있다.

[0059] 도 6은 본 발명의 실시 예에 따른 난수 발생기에 대한 제 4 실시 예를 보여주는 도면이다. 도 6을 참조하면, 제 1 발진기(410)의 고속 신호(S_F)가 제 2 발진기(420)의 중속 신호(S_M)의 여러 번 지연된 신호들에 의해 샘플될 것이다. 이는 1 → 0 및 0 → 1 변이들에 가까운 제 1 발진기(410)의 발진 신호(S_F)를 샘플링 할 기회를 증가시킬 수 있다. 이로써, 엔트로피가 증가될 것이다.

[0060] 본 발명의 실시 예에 따른 난수 발생기(400)는 하나의 고속 신호(S_F)를 중속 신호(S_M) 및 그것의 적어도 하나의 지연 신호들에 응답하여 제 1 샘플링(혹은, 프리 샘플링)을 수행하고, 제 1 샘플링된 결과값들 중에서 어느 하나를 선택하고, 선택된 값을 저속 신호인 샘플링 클록(SCK) 응답하여 제 2 샘플링(혹은, 메인 샘플링)을 수행한다.

[0061] 도 6에서는 복수의 엔트로피 소스들을 얻기 위하여 하나의 중속 신호(SM)를 지연시켰다. 하지만, 본 발명이 반드시 여기에 제한되지 않을 것이다. 본 발명은 복수의 엔트로피 소스들을 얻기 위하여 복수의 중속 신호(S_M)를 발생하기 위하여 복수의 중속 발진기들을 사용할 수 있다.

[0062] 도 7은 본 발명의 실시 예에 따른 난수 발생기에 대한 제 5 실시 예를 보여주는 도면이다. 도 7을 참조하면, 등가 분포된 제 1 발진기(510)의 발진 신호(S_F)를 샘플링하는 것으로 좀 더 높은 엔트로피를 유도하기 위하여 높은 지터를 갖는 복수의 제 2 발진기들(520_1, 520_2, 520_3)이 사용된다. 제 2 발진기들(520_1, 520_2, 520_3)의 주파수는 코-프라임 값들로 선택될 수 있다. 복수의 제 2 발진기들(520_1, 520_2, 520_3)의 사용은, 1 → 0 및 0 → 1 변이들에 가까운 제 1 발진기(410)의 발진 신호(S_F)를 샘플링 할 기회를 증가시킴으로써, 발생된 난수들의 품질을 증가시킬 수 있다.

[0063] 도 1 내지 도 7은 하나의 난수 비트를 출력하였다. 그러나 본 발명의 난수 발생기가 반드시 여기에 제한되지 않을 것이다. 본 발명의 난수 발생기는 복수의 난수 비트들을 출력할 수 있다.

[0064] 도 8은 본 발명의 실시 예에 따른 난수 발생기에 대한 제 6 실시 예를 보여주는 도면이다. 도 8를 참조하면, 난수 발생기(600)는 중속 발진기들(620_1, 620_2, 620_3)의 출력들을 배타적 논리합(XORing)하는 것을 제외하고 도 8에 도시된 난수 발생기(500)과 유사하다. 난수 발생기(600)는 병렬로 샘플된 값들을 출력할 것이다.

[0065] 만일, 중속 발진기들(620_1, 620_2, 620_3)의 모든 위상 값들이 임의이고 독립적이라면, 병렬 비트들의 마지막으로 발생된 값들은 임의이고 독립적이다. 따라서, 이러한 스킴은 난수 발생기의 성능을 증가시킨다.

[0066] 도 9는 본 발명의 실시 예에 따른 난수 발생기를 갖는 암호 프로세서를 포함하는 보안 시스템(1000)을 예시적으로 보여주는 블록도이다. 도 9를 참조하면, 보안 시스템(1000)은 중앙처리장치(1100), 암호 프로세서(1200), 롬(1300), 램(1400), 및 암호 프로세서용 메모리(1500)를 포함한다.

[0067] 중앙처리장치(1100)는 보안 시스템(1000)의 전반적인 동작을 제어한다. 암호 프로세서(1200)는 중앙처리장치(1100)의 제어에 따라 암호, 인증 및 전자 서명을 가능하게 하는 명령을 해독하고, 데이터를 처리한다. 암호 프로세서(1200)는 도 1 내지 도 8에서 설명된 난수 발생기를 포함한다.롬(1300)과 램(1400)은 보안 시스템(1000)을 구동하는데 필요한 데이터를 저장한다. 암호 프로세서용 메모리(1500)는 암호 프로세서(1200)의 구동에 필요한 데이터를 저장한다.

[0068] 한편, 본 발명의 상세한 설명에서는 구체적인 실시 예에 관하여 설명하였으나, 본 발명의 범위에서 벗어나지 않

는 한도 내에서 여러 가지로 변형할 수 있다. 그러므로 본 발명의 범위는 상술한 실시 예에 국한되어 정해져서는 안되며 후술하는 특허 청구범위뿐만 아니라 이 발명의 특허청구범위와 균등한 것들에 의해 정해져야 한다.

부호의 설명

[0069] 100, 200, 300, 400, 500, 600: 난수 발생기

110: 제 1 발진기

120: 제 2 발진기

130: 제 3 발진기 및 제어부

140, 240, 340, 440, 540: 샘플링부

151, 152: 듀티 싸이클 교정기

F_H: 고속 주파수

F_M: 중속 주파수

F_S: 저속 주파수

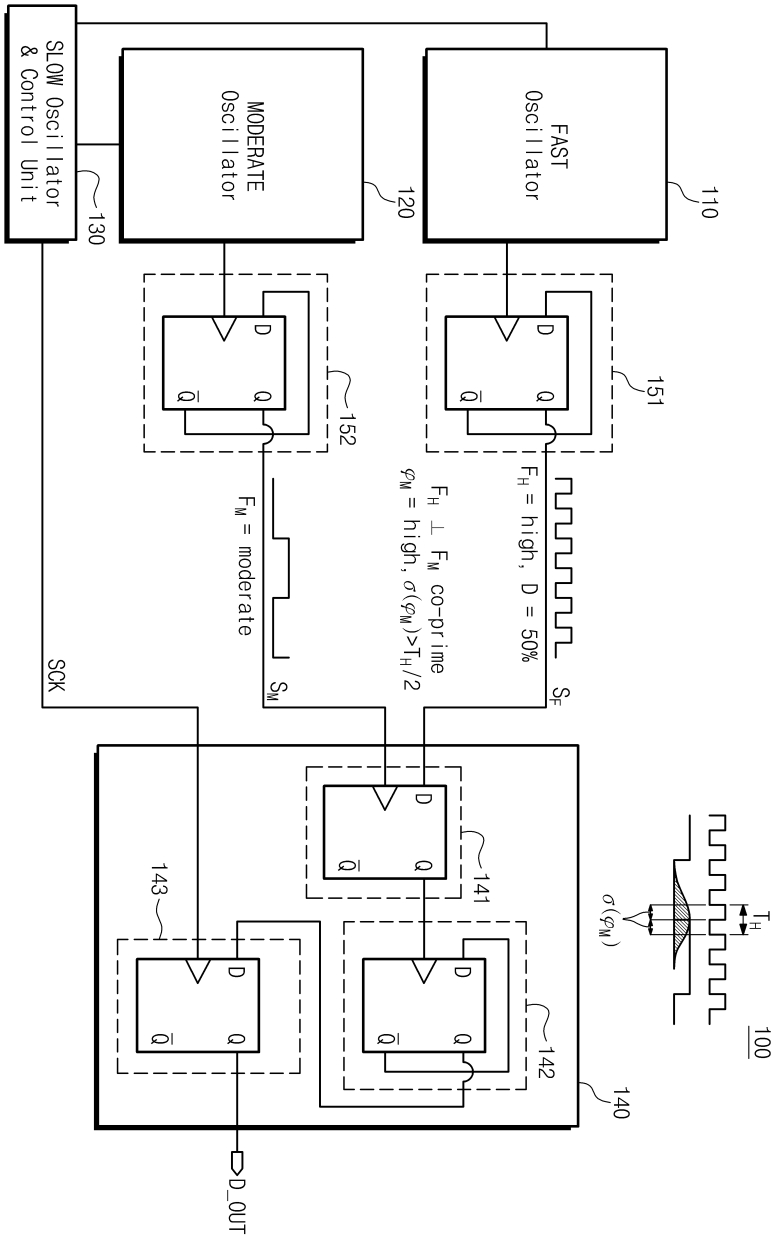
SCK: 샘플링 클록

S_F: 고속 신호

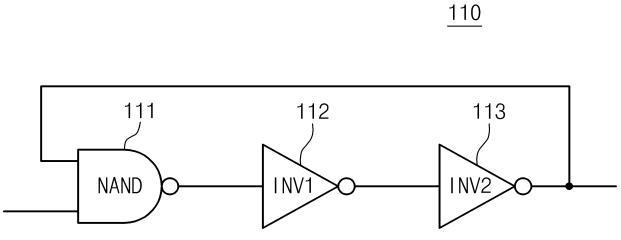
S_M: 중속 신호

도면

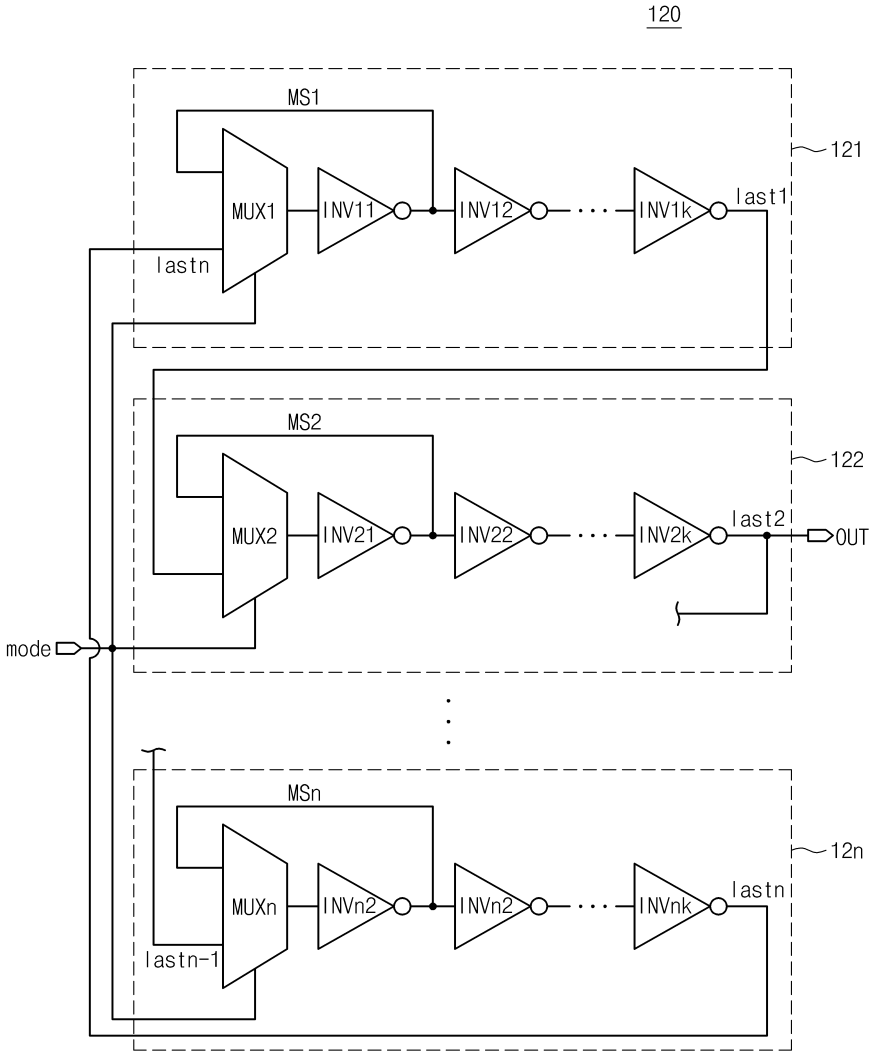
도면1


SLOW Oscillator & Control Unit
130
MODERATE Oscillator
120
FAST Oscillator
110
D
Q
152
151
SCK
F_M = moderate
S_M
$F_H \perp F_M$ co-prime
φ_M = high, $\sigma(\varphi_M) > T_H/2$
F_H = high, D = 50%
S_F
141
143
142
140
D_OUT
$\sigma(\varphi_M)$
T_H
100

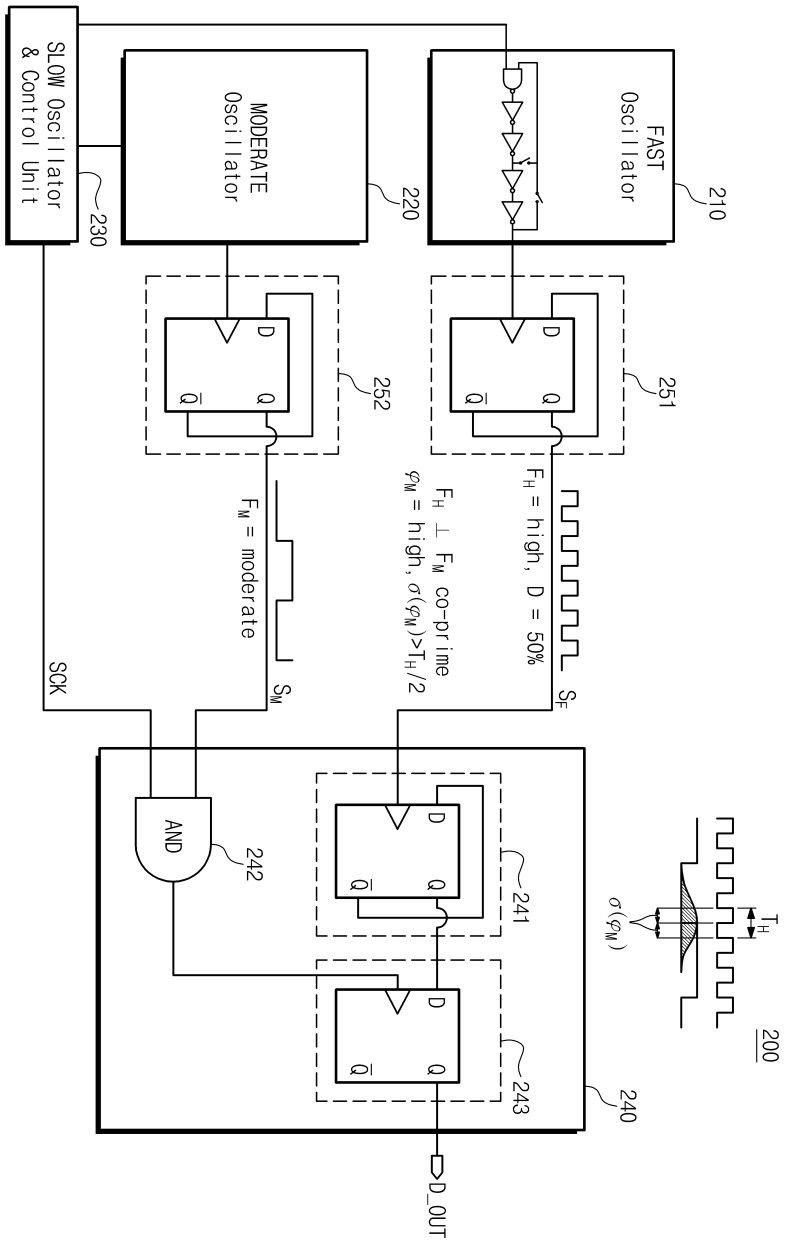
도면2


110
111
112
113
NAND
INV1
INV2

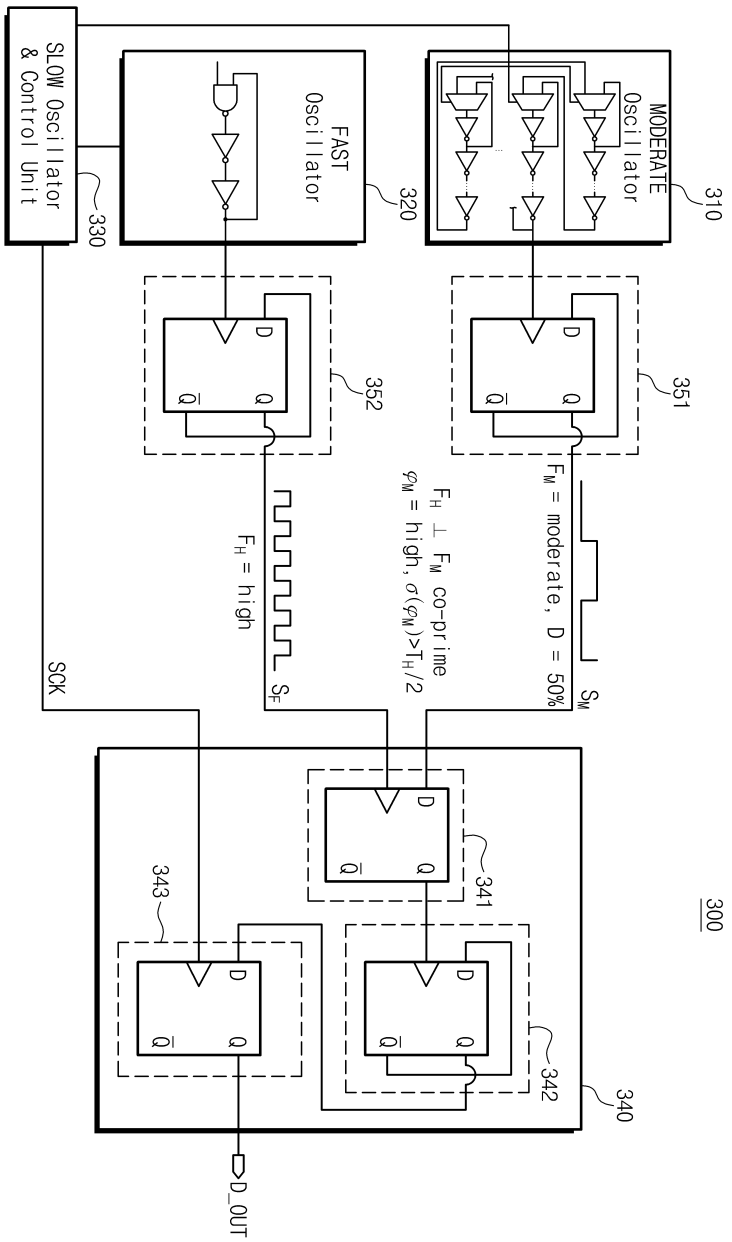
도면3


120
MS1
121
MUX1
INV11
INV12
INV1k
last1
lastn
MS2
122
MUX2
INV21
INV22
INV2k
last2
OUT
mode
MSn
12n
MUXn
INVn2
INVn2
INVnk
lastn
lastn-1

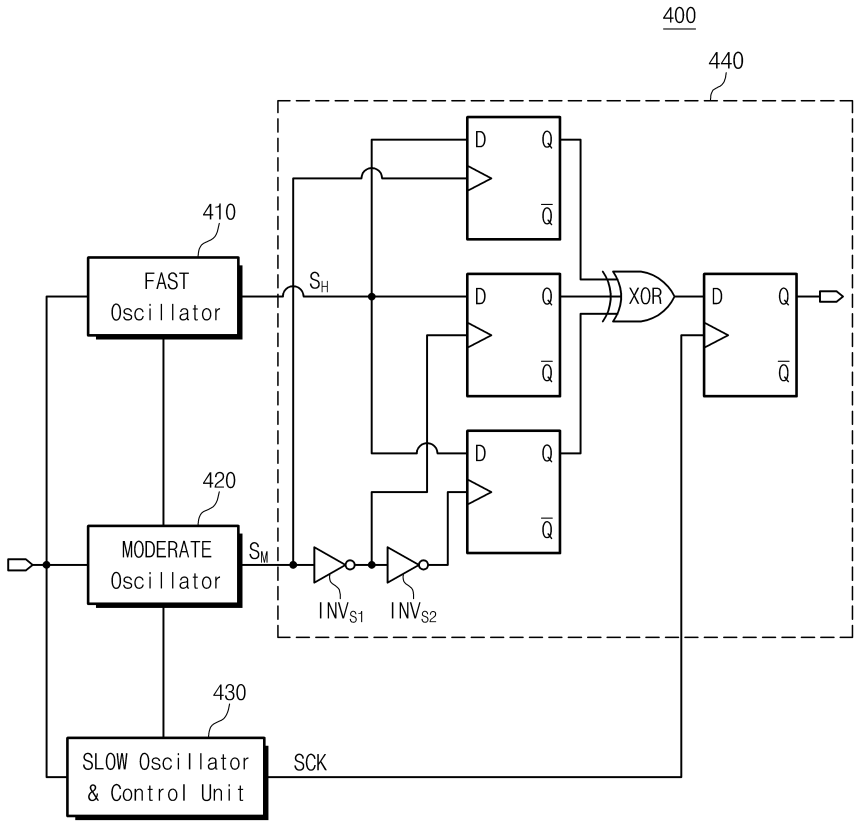
도면4


SLOW Oscillator & Control Unit
230
MODERATE Oscillator
220
FAST Oscillator
210
D
Q
252
251
F_M = moderate
S_M
$F_H \perp F_M$ co-prime
φ_M = high, $\sigma(\varphi_M) > T_H/2$
F_H = high, D = 50%
S_F
SCK
AND
242
241
243
240
D_OUT
$\sigma(\varphi_M)$
T_H
200

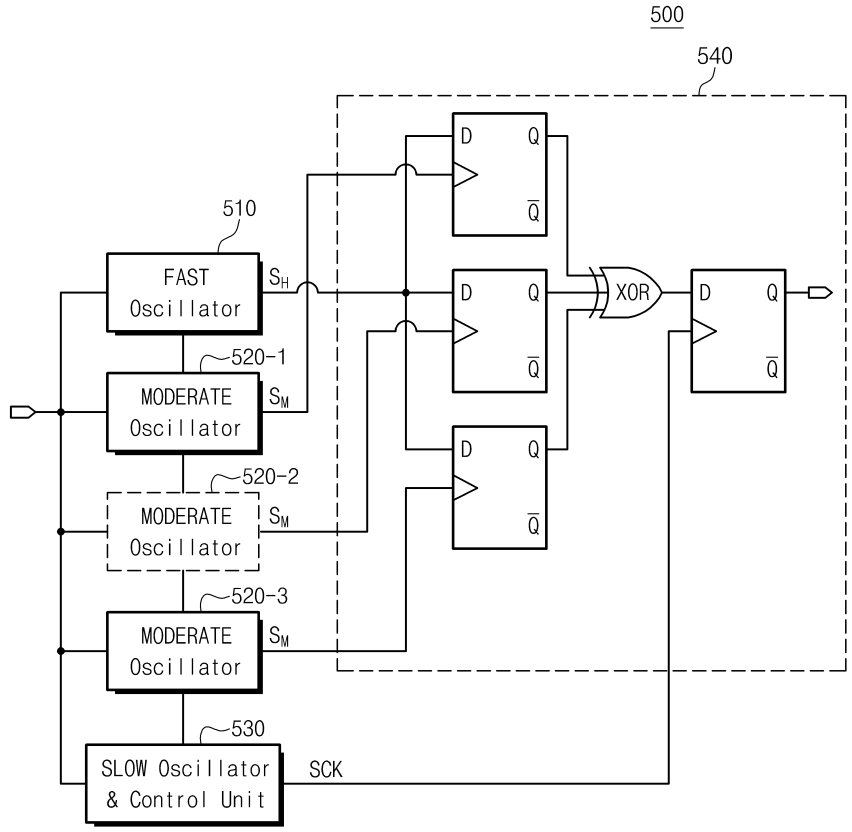
도면5


SLOW Oscillator & Control Unit
330
FAST Oscillator
320
MODERATE Oscillator
310
D
Q
352
351
F_H = high
S_F
$F_H \perp F_M$ co-prime
φ_M = high, $\sigma(\varphi_M) > T_H/2$
F_M = moderate, D = 50%
S_M
SCK
341
343
342
340
300
D_OUT

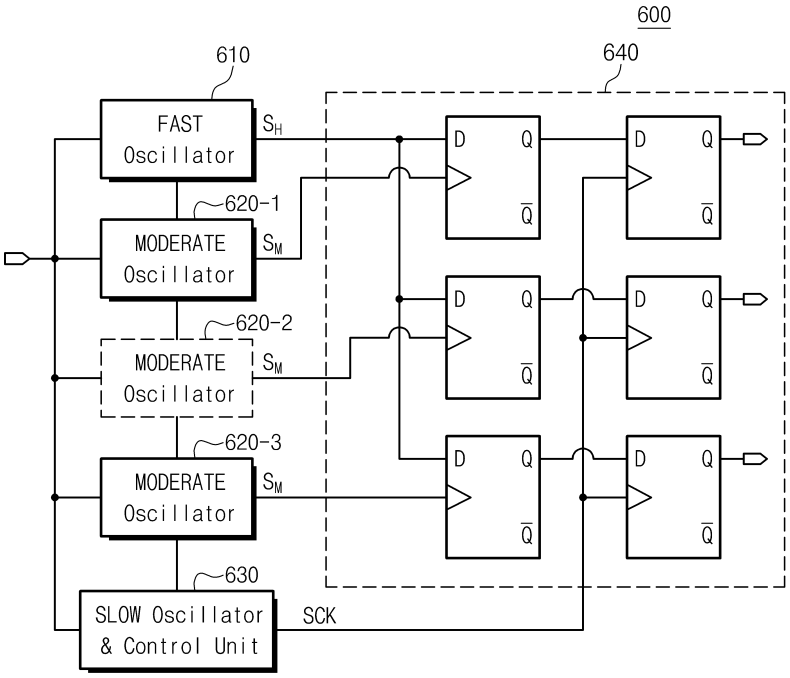
도면6


400
440
410
FAST
Oscillator
S_H
420
MODERATE
Oscillator
S_M
INV_{S1}
INV_{S2}
430
SLOW Oscillator
& Control Unit
SCK
D
Q
$\overline{Q}$
XOR

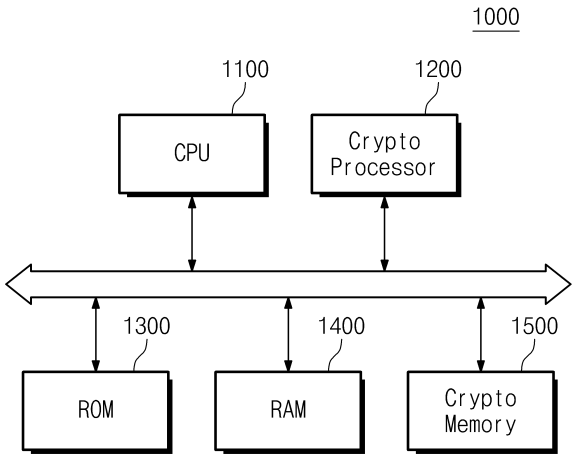
도면7


500
540
510
FAST
Oscillator
S_H
520-1
MODERATE
Oscillator
S_M
520-2
MODERATE
Oscillator
S_M
520-3
MODERATE
Oscillator
S_M
530
SLOW Oscillator
& Control Unit
SCK
D
Q
$\overline{Q}$
XOR

도면8



도면9



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 제5항

【변경전】

상기 발진 모드에서

【변경후】

발진 모드에서