(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2021-0115792
(43) 공개일자 2021년09월27일

(51) 국제특허분류(Int. Cl.)
G06F 21/72 (2013.01) *H04L 9/06* (2006.01)
(52) CPC특허분류
G06F 21/72 (2013.01)
H04L 9/06 (2013.01)
(21) 출원번호 10-2020-0032097
(22) 출원일자 2020년03월16일
심사청구일자 2020년03월16일

(71) 출원인
국방과학연구소
대전광역시 유성구 북유성대로488번길 160 (수남동)
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
김보훈
서울특별시 성북구 고려대로11길 66, 103호 (안암동1가)
박종선
서울특별시 서초구 신반포로 9, 85동 403호 (반포동, 반포아파트)
(뒷면에 계속)
(74) 대리인
제일특허법인(유)

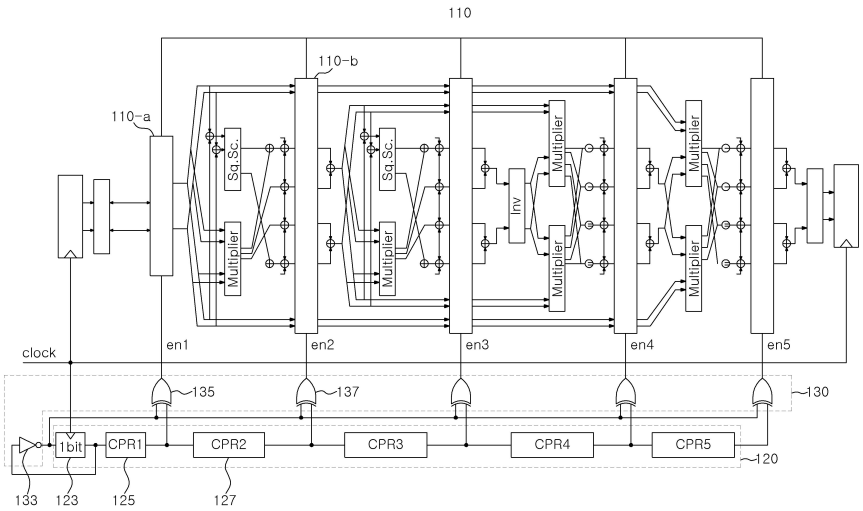
전체 청구항 수 : 총 6 항

(54) 발명의 명칭 **에스-박스의 임계화 구현을 위한 동기화 회로**

(57) 요 약

일 실시예에 따른 동기화 회로에 있어서, 활성화 신호를 생성하는 활성화 신호 생성부; 및 암호화 회로에 포함되어서 입력받은 신호의 비트를 상기 입력받은 신호의 비트수 이상의 비트로 나누어 연산하는 임계화 구현 연산을 수행하는 S-box 내부에 위치하며, 상기 생성된 활성화 신호에 기초해서, 상기 임계화 구현 연산과정에서 사용되는 신호들을 동기화시키는 동기화부를 포함할 수 있다.

대 표 도



(72) 발명자

김동화

대전광역시 유성구 북유성대로488번길 160 (수남동)

안명길

대전광역시 유성구 북유성대로488번길 160 (수남동)

명 세 서

청구범위

청구항 1

활성화 신호를 생성하는 활성화 신호 생성부; 및

암호화 회로에 포함되어서 입력받은 신호의 비트를 상기 입력받은 신호의 비트수 이상의 비트로 나누어 연산하는 임계화 구현 연산을 수행하는 S-box 내부에 위치하며, 상기 생성된 활성화 신호에 기초해서, 상기 임계화 구현 연산과정에서 사용되는 신호들을 동기화시키는 동기화부를 포함하는

동기화 회로.

청구항 2

제 1 항에 있어서,

상기 활성화 신호를 제공받은 동기화부에 초기화 신호를 제공하는 초기화 회로부를 포함하는

동기화 회로.

청구항 3

제 1 항에 있어서,

상기 동기화부는,

상기 입력 신호의 일부 및 상기 활성화 신호를 입력 받는 AND 게이트 복수 개; 및

상기 AND 게이트 복수 개 각각의 출력을 입력 받는 제 1 XOR 게이트를 포함하는 조합 논리 회로부 복수 개를 포함하는

동기화 회로.

청구항 4

제 1 항에 있어서,

상기 활성화 신호 생성부는,

클럭 신호를 입력 받는 플립플롭;

상기 플립플롭의 출력 신호를 제공 받고, 상기 동기화부 중 일부에 상기 활성화 신호를 제공하는 제 1 임계 경로 복제 회로부(Critical Path Replica circuit); 및

상기 제 1 임계 경로 복제 회로부와 직렬 연결되며, 상기 동기화 회로 중 일부와 다른 동기화 회로에 상기 활성화 신호를 제공하는 제 2 임계 경로 복제 회로부(Critical Path Replica circuit) 를 포함하는,

동기화 회로.

청구항 5

제 2 항에 있어서,

상기 초기화 회로부는,

상기 플립플롭의 출력 신호를 입력 받는 NOT 게이트;

상기 NOT 게이트의 출력 신호와 상기 제 1 임계 경로 복제 회로부의 출력신호를 입력 받는 제 2 XOR 게이트; 및

상기 NOT 게이트의 출력 신호와 상기 제 2 임계 경로 복제 회로부의 출력신호를 입력 받는 제 3 XOR 게이트를 포함하는

동기화 회로.

청구항 6

제 1 항에 있어서,

상기 동기화부는,

상기 활성화 신호를 제공 받아 선택적으로 스위칭 되는 제 1 스위치 소자;

상기 제 1 스위치 소자와 직렬 연결되며, 상기 입력 신호를 제공 받는 상단 회로(PUN, pull-up network);

상기 상단 회로(PUN)와 직렬 연결되며, 상기 입력 신호를 제공 받는 하단 회로(PDN, pull-down network); 및

상기 상단 회로(PUN)와 직렬 연결되고, 상기 하단 회로(PDN)와는 병렬 연결되며, 상기 활성화 신호를 제공 받아 선택적으로 스위칭 되는 제 2 스위치 소자를 포함하는

동기화 회로.

발명의 설명

기 술 분 야

[0001] 본 발명은 암호화 회로의 S-box에서 수행되는 임계화 구현 연산과정에서 사용되는 신호들을 동기화 시키기 위한 동기화 회로에 관한 것이다.

배 경 기 술

[0002] AES(Advanced Encryption Standard)와 같은 암호화 회로에서 악의적인 공격자는 키(key)값과 같은 민감한 정보를 탈취해 갈 수 있다.

[0003] 특히, 공격자의 공격 방법 중, 부채널 공격(SCA, Side Channel Attack)은 알고리즘에 직접 관여하지 않고 알고리즘이 동작하는 동안 발생하는 전자파나 소비 전력 등의 부가 정보를 이용하는 공격 방법인데 그 중에서도 입력 데이터와 소비 전력 간의 상관 관계를 분석하여 공격에 이용하는 차분전력 분석(DPA, Differential Power Analysis) 또는 상관관계전력분석(CPA, Correlation Power Analysis)은 강력한 공격능력으로 인해 널리 쓰이고 있다.

[0004] 이러한 공격자의 공격을 막기 위한 방법으로, 연산 과정에서 중간 값을 랜덤 값과 결합시킴으로써 연산 알고리즘과 실제 연산되는 값 사이의 상관관계를 제거하는 마스킹(Masking) 기법이 제안되었다.

[0005] 하지만, 회로상에서 신호가 도달하는 딜레이(delay) 차이에 의해 글리치(glitch) 현상이 발생함에 따라 발생하는 전력 소모를 이용하면 마스킹(Masking)이 적용된 회로에 대해서도 여전히 전력 분석이 가능한 문제점이 발생하였다.

[0006] 이에 대하여, 글리치(glitch) 문제를 해결하기 위해 발전된 마스킹 기법인 TI(Threshold Implementation)가 제안되었으며, TI(Threshold Implementation)는 입력된 비트(bit)를 여러 비트(bit)로 나누어 연산하는 기법으로, 기존의 함수 또한 여러 개의 보조함수로 나누어서 설계된다.

[0007] 다만, TI(Threshold Implementation)에서 암호 알고리즘에 사용되는 비선형 연산인 m비트 입력을 n비트 출력으로 변환하는 치환(substitution) 연산을 수행하는 S-box에서는 AND 연산(곱셈 연산)이 포함되는 구간(stage)마다 신호를 동기화(synchronization)시켜야만 글리치(glitch) 현상에서 발생되는 정보의 누출을 방지할 수 있었다.

선행기술문헌

특허문헌

[0008] (특허문헌 0001) 한국등록특허공보, 10-1631680호 (2016.06.13. 등록)

발명의 내용

해결하려는 과제

[0009] 본 발명의 해결하고자 하는 과제는, 동기화 회로를 제공하는 것이다.

[0010] 또한, 단순한 회로 구성만으로 S-box에서 수행되는 임계화 구현 연산과정에서 사용되는 신호들을 동기화 시킬 수 있으며, 이에 따라 상대적으로 동기화 회로를 구현하기 위한 면적, 전력 소모량 및 비용을 절감 하는 것 등이 본 발명의 해결하고자 하는 과제에 포함될 수 있다.

[0011] 다만, 본 발명의 해결하고자 하는 과제는 이상에서 언급한 것으로 제한되지 않으며, 언급되지 않은 또 다른 해결하고자 하는 과제는 아래의 기재로부터 본 발명이 속하는 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0012] 일 실시예에 따른 동기화 회로는, 활성화 신호를 생성하는 활성화 신호 생성부; 및 암호화 회로에 포함되어서 입력받은 신호의 비트를 상기 입력받은 신호의 비트수 이상의 비트로 나누어 연산하는 임계화 구현 연산을 수행하는 S-box 내부에 위치하며, 상기 생성된 활성화 신호에 기초해서, 상기 임계화 구현 연산과정에서 사용되는 신호들을 동기화시키는 동기화부를 포함할 수 있다.

[0013] 또한, 상기 활성화 신호를 제공받은 동기화부에 초기화 신호를 제공하는 초기화 회로부를 포함할 수 있다.

[0014] 또한, 상기 동기화부는, 상기 입력 신호의 일부 및 상기 활성화 신호를 입력 받는 AND 게이트 복수 개; 및 상기 AND 게이트 복수 개 각각의 출력을 입력 받는 제 1 XOR 게이트를 포함하는 조합 논리 회로부 복수 개를 포함할 수 있다.

[0015] 또한, 상기 활성화 신호 생성부는, 클럭 신호를 입력 받는 플립플롭; 상기 플립플롭의 출력 신호를 제공 받고, 상기 동기화부 중 일부에 상기 활성화 신호를 제공하는 제 1 임계 경로 복제 회로부(Critical Path Replica circuit); 및 상기 제 1 임계 경로 복제 회로부와 직렬 연결되며, 상기 동기화 회로 중 일부와 다른 동기화 회로에 상기 활성화 신호를 제공하는 제 2 임계 경로 복제 회로부(Critical Path Replica circuit)를 포함할 수 있다.

[0016] 또한, 상기 초기화 회로부는, 상기 플립플롭의 출력 신호를 입력 받는 NOT 게이트; 상기 NOT 게이트의 출력 신호와 상기 제 1 임계 경로 복제 회로부의 출력신호를 입력 받는 제 2 XOR 게이트; 및 상기 NOT 게이트의 출력 신호와 상기 제 2 임계 경로 복제 회로부의 출력신호를 입력 받는 제 3 XOR 게이트를 포함할 수 있다.

[0017] 또한, 상기 동기화부는, 상기 활성화 신호를 제공 받아 선택적으로 스위칭 되는 제 1 스위치 소자; 상기 제 1 스위치 소자와 직렬 연결되며, 상기 입력 신호를 제공 받는 상단 회로(PUN, pull-upnetwork); 상기 상단 회로(PUN)와 직렬 연결되며, 상기 입력 신호를 제공 받는 하단 회로(PDN, pull-down network); 및 상기 상단 회로(PUN)와 직렬 연결되고, 상기 하단 회로(PDN)와는 병렬 연결되며, 상기 활성화 신호를 제공 받아 선택적으로 스위칭 되는 제 2 스위치 소자를 포함할 수 있다.

발명의 효과

[0018] 일 실시예에 따른 동기화 회로는 단순한 조합 논리 회로 또는 스위치 소자를 사용하여 S-box에서 수행되는 임계화 구현 연산과정에서 사용되는 신호들을 동기화시킬 수 있으므로, 상대적으로 동기화 회로를 구현하기 위한 면적, 전력 소모량 및 비용을 절감시킬 수 있다.

[0019] 또한, 동기화 회로는 여러 클락 사이클(cycle)이 걸리는 연산을 한 클락 사이클(clcle) 안에 연산을 수행할 수 있기 때문에, 연산의 지연(latency)을 크게 줄일 수 있다.

[0020] 또한, 동기화 회로를 사용함으로써 회로상에서 신호가 도달하는 딜레이(delay) 차이에 의해 발생되는 글리치(glitch) 현상이 제거될 수 있다.

도면의 간단한 설명

[0021] 도 1은 일 실시예에 따른 동기화 회로의 회로도이다.

도 2는 일 실시예에 따른 동기화부의 회로도이다.

도 3은 또 다른 실시예에 대한 일 실시예에 따른 동기화부의 회로도이다.

도 4는 일 실시예에 따른 초기화 회로부에 대한 신호 파형이다.

발명을 실시하기 위한 구체적인 내용

[0022] 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나 본 발명은 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하고, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다.

[0023] 본 발명의 실시예들을 설명함에 있어서 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다. 그리고 후술되는 용어들은 본 발명의 실시예에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

[0024] 도 1은 일 실시예에 따른 동기화 회로(100)의 회로도이다.

[0025] 일 실시예에 따른 동기화 회로(100)는 암호화 회로에서 입력받은 신호의 비트를 입력 받은 신호의 비트수 이상의 비트로 나누어 연산하는 임계화 구현(Threshold Implementation) 연산을 수행하는 S-box에서 수행되는 임계화 구현 연산과정에서 사용되는 신호들을 동기화 시키기 위한 회로일 수 있으나 이에 한정되는 것은 아니다.

[0026] 도 1을 참조하면, 일 실시예에 따른 동기화 회로(100)는 동기화부(110), 활성화 신호 생성부(120) 및 초기화 회로부(130)를 포함할 수 있으나, 이에 한정되는 것은 아니다. 아울러, 이러한 동기화 회로(100)에 포함된 구성 각각은 소프트웨어 모듈이나 하드웨어 모듈 형태로 구현되거나 또는 소프트웨어 모듈과 하드웨어 모듈이 조합된 형태, 예컨대 컴퓨터나 스마트 기기 등에서 구현될 수 있고, 각각의 구성들은 전기적으로 연결될 수 있다.

[0027] 동기화부(110)는 암호화 회로에 포함되어서 입력받은 신호의 비트를 상기 입력 받은 신호의 비트수 이상의 비트로 나누어 연산하는 임계화 구현(Threshold Implementation) 연산을 수행하는 S-box 내부에 위치하며, 활성화 신호에 기초해서, 상기 임계화 구현 연산과정에서 사용되는 신호들을 동기화시킬 수 있다.

[0028] 여기서, 입력 받은 신호는 S-box에서 연산되는 신호 중 적어도 일부의 신호 일 수 있으며, 활성화 신호는 후술할 활성화 신호 생성부(120)를 통해 제공 받을 수 있다.

[0029] 보다 상세히, 동기화부(110)는 후술할 활성화 신호 생성부(120)를 통해 활성화 신호(EN, Enable signal)를 공급받아 S-box에서 수행되는 임계화 구현 연산과정에서 사용되는 신호들을 동기화 시킬 수 있다.

[0030] 즉, 동기화부(110)는 활성화 신호 생성부(120)로부터 공급 받은 활성화 신호에 기초하여 S-box에서 수행되는 임계화 구현 연산과정에서 사용되는 신호들을 동기화 시킬 수 있다.

[0031] 이하, 동기화부(110)의 실시예에 대하여 도 2 및 도 3을 통해 상세히 설명하도록 한다.

[0032] 도 2는 일 실시예에 따른 동기화부(110)의 회로도이다.

[0033] 도 2를 참조하면, 동기화부(110)는 조합 논리 회로부(115)를 포함할 수 있으며, 조합 논리 회로부(115)는 복수개일 수 있다.

[0034] 조합 논리 회로부(115)는 복수의 AND 게이트(113a, 113b) 및 제 1 XOR 게이트(114) 를 포함할 수 있다.

[0035] 복수의 AND 게이트(113a, 113b)는 S-box에서 연산되는 신호 중 적어도 일부의 신호(In1, In2)와 활성화 신호(En)를 입력 받아 AND 연산하여 출력할 수 있다.

[0036] 이때, 복수의 AND 게이트는 후술할 활성화 신호 생성부(120)로부터 활성화 신호(En)를 제공받을 수 있으나 이에 한정되는 것은 아니다.

[0037] 제 1 XOR 게이트(114)는 복수의 AND 게이트(113a, 113b) 각각에서 출력되는 신호를 입력 받아 XOR 연산하여 출력할 수 있다.

[0038] 예를 들어, 제 1 XOR 게이트(114)는 113a의 AND 게이트에서 출력되는 신호 및 113b의 AND 게이트에서 출력되는

신호를 입력 받아 XOR 연산하여 출력할 수 있다.

[0039] 도 3은 또 다른 실시예에 대한 일 실시예에 따른 동기화부(110)의 회로도이다.

[0040] 도 3의 (a)는 또 다른 실시예에 대한 일 실시예에 따른 동기화 부(110)의 개념을 설명하기 위한 회로도이다.

[0041] 도 3의 (a)를 참조하면, 동기화부(110)는 AND 게이트를 포함하지 않고, 입력 신호(In1, In2, 예컨대 S-box에서 연산되는 신호 중 적어도 일부의 신호) 및 활성화 신호(En, enable signal)를 입력 받아 XOR 연산하여 출력할 수 있다.

[0042] 즉, 도 3의 (a)에 도시된 XOR 게이트는 S-box에서 연산되는 신호 중 적어도 일부의 신호(In1, In2) 및 활성화 신호(En, enable signal)를 입력 받아 XOR 연산하여 출력할 수 있다.

[0043] 도 3의 (b)를 참조하면, 도 3의 (b)에 도시된 동기화부(110)는 제 1 스위치 소자(300), 상단 회로(310, PUN: pull-upnetwork), 하단 회로(320, PDN: pull-down network) 및 제 2 스위치 소자(330)를 포함할 수 있다.

[0044] 예컨대, 도 3의 (b)의 회로는 암호화 회로의 CMOS(Complementary metal-oxide-semiconductor) 기반의 구조에서 제 1 스위치 소자(300) 및 제 2 스위치 소자(330)을 추가하여 구현할 수 있다.

[0045] 한편, 도 3의 (b)에 도시된 동기화부(110)는 암호화 알고리즘 구현에 사용되는 표준 셀(standard cell) 대신 사용될 수 있으나 이에 한정되는 것은 아니다.

[0046] 제 1 스위치 소자(300)는 활성화 신호(En)를 공급 받아 선택적으로 스위칭 될 수 있다.

[0047] 상단 회로(310, PUN)는 제 1 스위치 소자(300)와 직렬 연결되며, 입력 신호(In1, In2, 예컨대 S-box에서 연산되는 신호 중 적어도 일부의 신호)를 제공받을 수 있다.

[0048] 하단 회로(320, PDN)는 상단 회로(310, PUN)와 직렬 연결되며, 입력 신호(In1, In2, 예컨대 S-box에서 연산되는 신호 중 적어도 일부의 신호)를 제공받을 수 있다.

[0049] 여기서, 상단 회로(310, PUN) 및 하단 회로(320, PDN)가 제공 받는 신호는 동일한 신호일 수 있다.

[0050] 제 2 스위치 소자(330)는 상단 회로(310, PUN)와 직렬 연결되고, 하단 회로(320, PDN)와는 병렬 연결되며, 활성화 신호(En)를 공급 받아 선택적으로 스위칭될 수 있다.

[0051] 예컨대, 제 1 스위치 소자(300) 및 제 2 스위치 소자(310)는 스위치가 턴온 또는 턴오프될 수 있는 스위칭 소자로서, 트랜지스터(Transistor) 등으로 구현될 수 있다

[0052] 한편, 도 3의 (b) 회로도는 도 3의 (a)와 같이 별도의 AND 게이트의 구성 없이, S-box에서 연산되는 신호 중 적어도 일부의 신호(In1, In2) 및 활성화 신호(En)를 공급받아 신호 처리할 수 있다.

[0053] 보다 상세히, 도 3의 (b) 회로도는 활성화 신호를 공급 받는 제 1 스위치 소자(300) 및 제 2 스위치 소자(330)가 선택적으로 스위칭됨으로써, 활성화 신호(En)의 공급 타이밍을 조절하고, 적절한 타이밍에 활성화 신호가 공급되어, 공급된 활성화 신호에 기초하여 S-box에서 연산되는 신호 중 적어도 일부의 신호(In1, In2)를 동기화시켜 출력(Out)할 수 있다.

[0054] 이와 같이, 동기화부(110)는 단순한 조합 논리 회로 또는 스위치 소자를 사용하여 설계될 수 있으므로, 동기화부(110)를 플립플롭(FF: Flip Flop)등으로 구현하는 것에 비해 연산되는 비트를 적게 쓸 수 있을 뿐만 아니라 동기화 부(110)를 구현하기 위한 면적, 전력 소모량 및 비용을 절감시킬 수 있다.

[0055] 한편, 다시 도 1을 참조하면, 활성화 신호 생성부(120)는 활성화 신호를 생성하고, 동기화 부(110)에 활성화 신호를 공급하도록 마련될 수 있다.

[0056] 이러한 활성화 신호 생성부(120)는 플립플롭(123), 제 1 임계 경로 복제 회로부(125, CPR1, Critical Path Replica circuit) 및 제 2 임계 경로 복제 회로부(127, CPR2, Critical Path Replica circuit)를 포함할 수 있다.

[0057] 플립플롭(123)은 클럭(clock) 신호를 입력 받아 동작될 수 있다.

[0058] 제 1 임계 경로 복제 회로부(125, CPR1)는 플립플롭(123)의 출력 신호를 제공 받고, 동기화부(110) 중 일부에 활성화 신호(en1)를 공급하도록 동작될 수 있다.

[0059] 예를 들어, 제 1 임계 경로 복제 회로부(125, CPR1)는 동기화부(110)의 복수의 조합 논리 회로 중 일부에 활성

화 신호(en1)를 공급하도록 동작될 수 있다.

[0060] 제 2 임계 경로 복제 회로부(127, CPR2)는 제 1 임계 경로 복제 회로부(125)와 직렬 연결되며, 제 1 임계 경로 복제 회로부(125)가 동기화 부(110) 중 일부(110-a)에 활성화 신호(en1)를 제공한 후, 상기 동기화 부(110) 중 일부와 다른 동기화 부(110-b)에 상기 활성화 신호를 공급(en2) 하도록 동작될 수 있다.

[0061] 더 나아가, 활성화 신호 생성부(120)는 제 2 임계 경로 복제 회로부(127, CPR2)와 직렬 연결되어 있는 복수의 임계 경로 복제 회로부(CPR3, CPR4, CPR5 …)를 더 포함할 수도 있다.

[0062] 예컨대, 제 1 임계 경로 복제 회로부(125, CPR1) 및 제 2 임계 경로 복제 회로부(127, CPR2)는 복수의 논리 게이트 또는 인버터체인(Inverter chain)으로 구현될 수 있다.

[0063] 이때, 제 1 임계 경로 복제 회로부(125, CPR1) 및 제 2 임계 경로 복제 회로부(127, CPR2)는 설계자에 따라 다양하게 설계될 수 있으며, 예를 들어 동기화 부(110)와 동일한 회로로 설계될 수도 있다.

[0064] 한편, 활성화 신호 생성부(120)는 제 1 임계 경로 복제 회로부(125, CPR1)를 통해 동기화부의 일부(110-a)에 활성화 신호를 공급하게 되면, 동기화부의 일부(110-a)는 S-box에서 연산되는 신호 중 적어도 일부의 신호를 공급받은 활성화 신호에 기초하여 동기화시키고, 동기화된 신호를 다음구간의 동기화부(110-b)에게 전달하게 된다.

[0065] 여기서, 다음 구간의 동기화부(110-b)는 제 1 임계 경로 복제 회로부(125)를 통해 활성화 신호를 공급 받은 동기화부의 일부(110-a)와 근접하게 위치되어서, 동기화부의 일부(110-a)의 신호를 입력 받는 동기화부(110-b)를 의미한다.

[0066] 이 경우, 다음구간의 동기화부(110-b)는 동기화부의 일부(110-a)의 게이트들에 모든 신호가 도달한 이후, 활성화 신호를 공급받아야 하는데, 다음구간의 동기화부(110-b)는 제 2 임계 경로 복제 회로부(127)를 통과한 이후, 활성화 신호를 공급 받기 때문에 적절한 타이밍에 활성화 신호(en2)를 공급받을 수 있게 된다.

[0067] 초기화 회로부(130)는 활성화 신호를 제공받은 동기화부(110)에 초기화 신호를 제공할 수 있으며, 초기화 회로부(130)는 NOT 게이트(133), 제 2 XOR 게이트(135) 및 제 3 XOR 게이트(137)를 포함할 수 있다.

[0068] NOT 게이트(133)는 플립플롭(123)의 출력 신호를 입력 받아 NOT 연산하여 출력할 수 있다.

[0069] 제 2 XOR 게이트(135)는 NOT 게이트(133)의 출력 신호와 제 1 임계 경로 복제 회로부(125)의 출력 신호를 입력받아 XOR연산하여 활성화 신호(en1)를 출력할 수 있다.

[0070] 제 3 XOR 게이트(137)는 NOT 게이트(133)의 출력 신호와 제 2 임계 경로 복제 회로부(127)의 출력 신호를 입력받아 XOR연산하여 활성화 신호(en2)를 출력할 수 있다.

[0071] 더 나아가, 초기화 회로부(130)는 NOT 게이트(133)의 출력 신호와 복수의 임계 경로 복제 회로부(CPR3, CPR4, CPR5 …)의 출력 신호를 입력 받는 복수의 XOR 게이트를 더 포함할 수도 있다.

[0072] 이하, 초기화 회로부(130)의 동작에 대하여 도 4를 참조하여 상세히 설명하도록 한다.

[0073] 도 4는 일 실시예에 따른 초기화 회로도에 대한 신호 파형이다.

[0074] 도 4를 참조하면, 클락신호(clock)의 한 주기(cycle)안에 활성화 신호(en1, en2, en3)의 논리 신호가 모두 "1"이 되어 출력되는 것을 확인할 수 있다.

[0075] 보다 구체적으로, 플립플롭(FF)이 클럭 신호를 입력 받아 플립플롭(FF)의 출력 신호를 입력 받은 제 1 임계 경로 복제 회로부(125)에서 신호를 출력하고, 제 2 XOR 게이트(135)는 플립플롭(FF)의 출력 신호 "1"이 NOT 게이트(133)에 입력되어 NOT 연산된 신호 "0"과 제 1 임계 경로 복제 회로부(125)의 신호를 입력 받아, XOR 연산 하여 활성화 신호(en1) "1"을 출력할 수 있다.

[0076] 마찬가지로, 제 3 XOR 게이트(137)는 플립플롭(FF)의 출력 신호 "1"이 NOT 게이트(133)에 입력되어 NOT 연산된 신호 "0"과 제 2 임계 경로 복제 회로부(127)의 신호를 입력 받아, XOR 연산하여 활성화 신호(en2) "1"을 출력할 수 있다.

[0077] 이때, 제 3 XOR 게이트(136)에서 활성화 신호(EN1, EN2) "1"이 출력되면, 활성화 신호들(en1, en2, en3)은 각각 동기화부(110) 중 일부에 공급될 수 있다.

[0078] 한편, 한 클락 사이클(400, cycle)안에 활성화 신호들(en1, en2, en3)이 공급 된 후, 다음 클락 사이클(410, cycle)에서도 활성화 신호들(en1, en2, en3)이 공급되기 위해서는 활성화 신호들(en1, en2, en3)이 "1"에서 다

시 "0"으로 초기화 되어야만 한다.

[0079] 이때, 초기화 회로부(130)는 다음 클락 사이클(410, cycle)에서 플립플롭(FF)의 출력 신호 "0"이 NOT 게이트(133)에 입력되어 NOT 연산된 신호 "1"과 제 1 임계 경로 복제 회로부(125)의 신호를 입력 받아, 활성화 신호(en1, en2, en3) "0"을 출력하면서, 활성화 신호를 초기화 시킬 수 있다.

[0080] 따라서, 다음 클락 사이클(410, cycle)에서 활성화 신호들(en1, en2, en3)은 초기화(reset)될 수 있으며, 이에 따라 활성화 신호들(en1, en2, en3)은 초기화 된 후, 다시 동기화부(110)의 일부에 활성화 신호를 공급할 수 있게 된다.

[0081] 이상에서 살펴본 바와 같이, 일 실시예에 따른 동기화 회로는 단순한 조합 논리 회로 또는 스위치 소자를 사용하여 S-box에서 수행되는 임계화 구현 연산과정에서 사용되는 신호들을 동기화시킬 수 있으므로, 상대적으로 동기화 회로를 구현하기 위한 면적, 전력 소모량 및 비용을 절감시킬 수 있다.

[0082] 또한, 동기화 회로는 여러 클락 사이클(cycle)이 걸리는 연산을 한 클락 사이클(clcle) 안에 연산을 수행할 수 있기 때문에, 연산의 지연(latency)을 크게 줄일 수 있다.

[0083] 또한, 동기화 회로를 사용함으로써 회로상에서 신호가 도달하는 딜레이(delay) 차이에 의해 발생되는 글리치(glitch) 현상이 제거될 수 있다.

[0084] 이상의 설명은 본 발명의 기술 사상을 예시적으로 설명한 것에 불과한 것으로서, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 본 발명의 본질적인 품질에서 벗어나지 않는 범위에서 다양한 수정 및 변형이 가능할 것이다. 따라서, 본 발명에 개시된 실시예들은 본 발명의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시예에 의하여 본 발명의 기술 사상의 범위가 한정되는 것은 아니다. 본 발명의 보호 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 균등한 범위 내에 있는 모든 기술사상은 본 발명의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

부호의 설명

[0085] 100: 동기화 회로

110: 동기화부

113a, 113b: 복수의 AND 게이트

114: 제 1 XOR 게이트

120: 활성화 신호 생성부

123: 플립플롭

125: 제 1 임계 경로 복제 회로부

127: 제 2 임계 경로 복제 회로부

130: 초기화 회로부

133: NOT 게이트

135: 제 2 XOR 게이트

137: 제 3 XOR 게이트

300: 제 1 스위치 소자

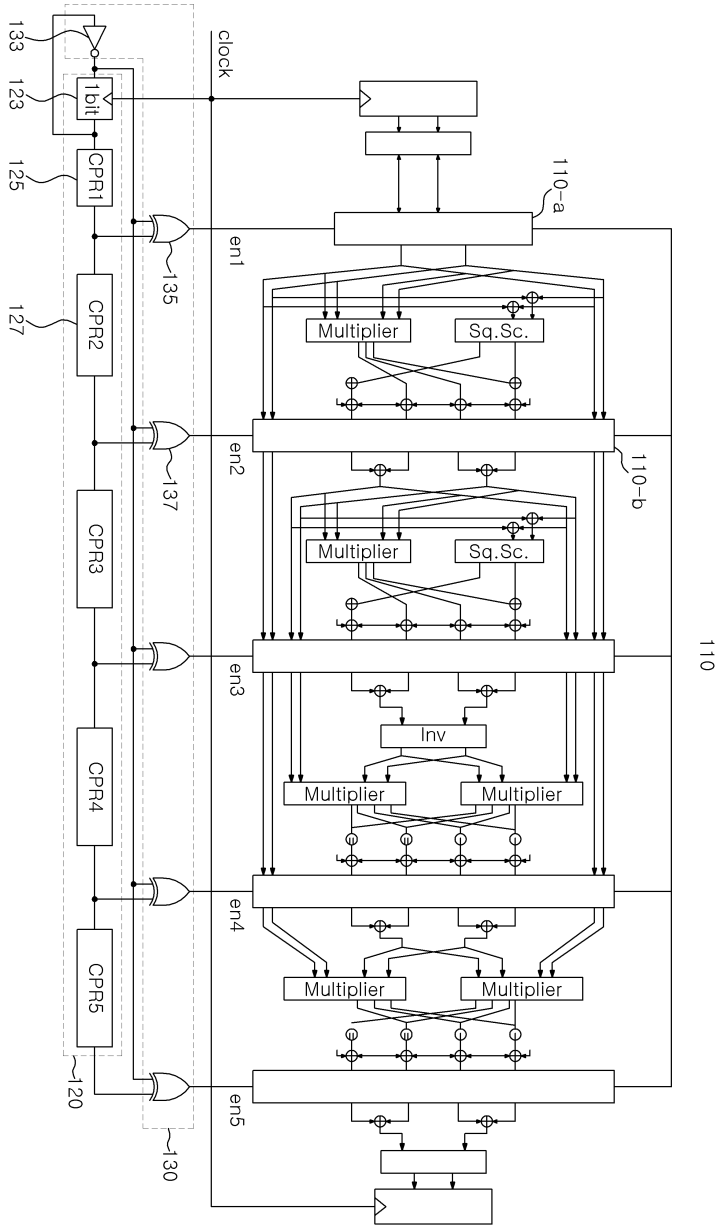
310: 상단 회로

320: 하단 회로

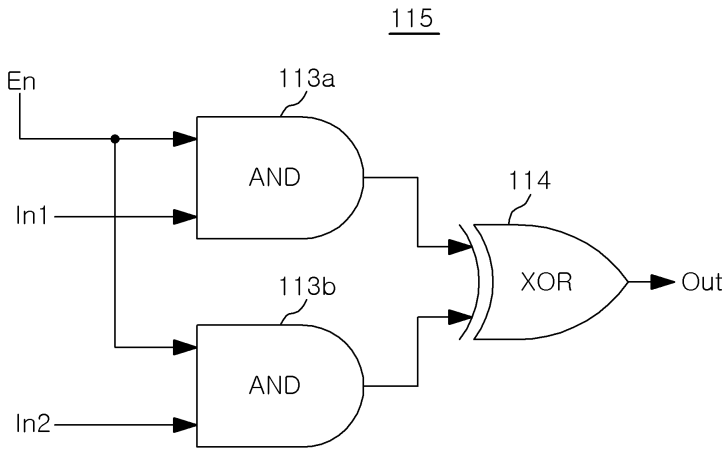
330: 제 2 스위치 소자

도면

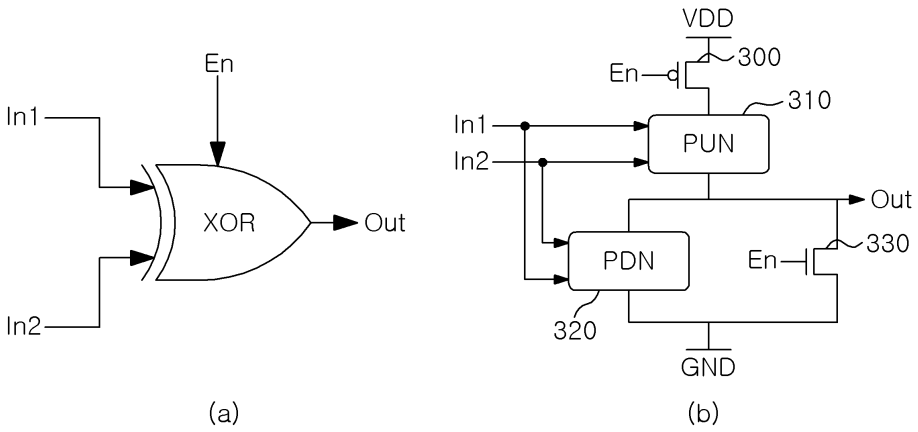
도면1


133
123
1bit
125
CPR1
127
CPR2
CPR3
CPR4
CPR5
120
130
clock
en1
135
en2
137
en3
en4
en5
110-a
110-b
110
Multiplier
Sq.Sc.
Inv

도면2


115
En
113a
AND
In1
114
XOR
Out
113b
AND
In2

도면3


En
In1
XOR
Out
In2
(a)
VDD
300
En
310
In1
PUN
In2
Out
PDN
En
330
320
GND
(b)

도면4

