(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2014 년 8 월 7 일 (07.08.2014)

WIPO | PCT

(10) 국제공개번호
WO 2014/119834 A1

(51) 국제특허분류:
H04L 12/861 (2013.01)

(21) 국제출원번호: PCT/KR2013/008109

(22) 국제출원일: 2013 년 9 월 9 일 (09.09.2013)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2013-0011450 2013 년 1 월 31 일 (31.01.2013) KR

(71) 출원인: **부산대학교 산학협력단 (PUSAN NATIONAL UNIVERSITY INDUSTRY--UNIVERSITY COOPERATION FOUNDATION)** [KR/KR]; 609-735 부산시 금정구 부산대학로 63 번길 2 (장전동, 부산대학교), Busan (KR).

(72) 발명자: **김호원 (KIM, Howon)**; 604-784 부산시 사하구 다대 1 동 1627 번지 롯데캐슬몰운대아파트 218 동 1603 호, Busan (KR). **이동건 (LEE, Donggeon)**; 607-060 부산시 동래구 온천동 SK 허브올리브 2505 호, Busan (KR). **최종석 (CHOI, Jongseok)**; 604-010 부산시 사하구 당리동 329-15 번지, Busan (KR).

(74) 대리인: **오위환 (OH, Wihwan)**; 135-080 서울시 강남구 역삼동 601-18 은성빌딩 5 층, Seoul (KR).

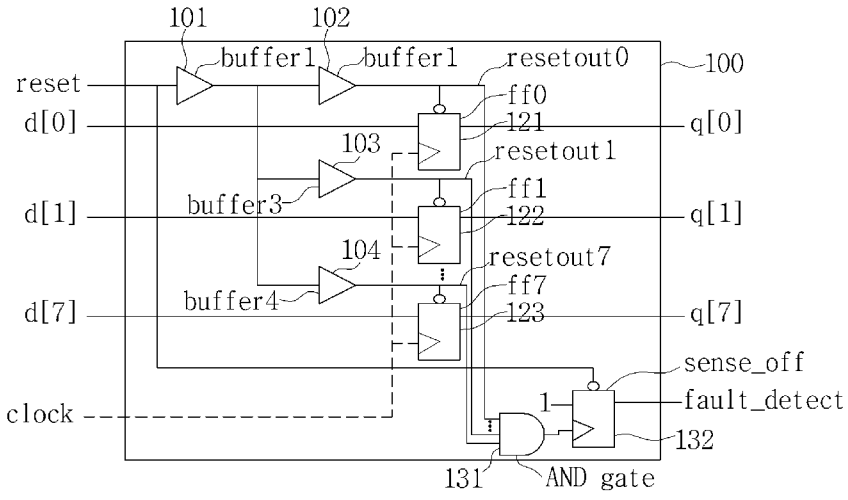
(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

[다음 쪽 계속]

(54) **Title**: CIRCUIT FOR DETECTING OPTICAL FAULT INJECTION USING BUFFERS ON RESET SIGNAL PATH

(54) **발명의 명칭** : 리셋 신호 경로상의 버퍼를 이용한 광학 오류 주입 탐지 회로



(57) **Abstract**: The present invention relates to a circuit for detecting an optical fault injection using buffers on a reset signal path required for resetting a chip, which includes: a plurality of sensors arranged on a reset signal path for delivering a reset signal to each of the flip-flops constituting a digital circuit so as to detect an external optical fault injection; a signal collection part for collecting the outputs of the sensors into one so as to distinguish a variation occurring in the signal of one of the sensors; and a detection signal generation part for generating a detection signal representing an optical fault injection according to the signal variation of the sensor inputted to the signal collection part.

(57) **요약서**: 본 발명은 칩을 리셋하기 위해 필요한 리셋 신호선 상에 존재하는 버퍼들을 이용하여 광학 오류 주입을 감지할 수 있도록 한 리셋 신호 경로상의 버퍼를 이용한 광학 오류 주입 탐지 회로에 관한 것으로, 디지탈 회로를 구성하는 각 플립플롭으로 전달되는 리셋 신호의 경로 상에 구성되어 외부의 광학 오류 주입을 감지하는 복수 개의 감지부;상기 감지부의 출력을 하나로 취합하여 어느 하나의 감지부의 신호에 변화가 발생하면 이를 구분하는 신호 취합부;상기 감지부에서 출력되는 신호 변화를 감지하여 신호 취합부의 입력에 의해 광학 오류 주입 탐지 신호를 발생시키는 탐지신호 발생부;를 포함하는 것이다.

WO 2014/119834 A1

공개:

— 국제조사보고서와 함께 (조약 제 21 조(3))

명세서

발명의 명칭: 리셋 신호 경로상의 버퍼를 이용한 광학 오류 주입 탐지 회로

기술분야

[1] 본 발명은 광학 오류 주입 공격 대응에 관한 것으로, 구체적으로 칩을 리셋하기 위해 필요한 리셋 신호선 상에 존재하는 버퍼들을 이용하여 광학 오류 주입을 감지할 수 있도록 한 리셋 신호 경로상의 버퍼를 이용한 광학 오류 주입 탐지 회로에 관한 것이다.

배경기술

[2] 일반적으로 네트워크 장치들에 사용되고 있는 암호 알고리즘들은 오류 주입 공격에 취약한 단점이 있다.

[3] 예를 들어, AES(Advanced Encryption Standard) 암호 알고리즘의 경우 키 스케쥴링이나 암호화가 수행되는 동안 데이터를 저장하는 레지스터나 메모리에 오류가 주입되어 정상 암호문과 오류 암호문의 차이 값을 이용한 차분오류 분석(Differential Fault Analysis)에 의해 비밀키 값이 누출되는 문제가 있다.

[4] RSA-CRT(Rivest Shamir Adleman-Chinese Remainder Theorem) 암호 알고리즘은 일반적인 RSA 암호 알고리즘에 비해서 연산의 효율성이 높고 전력 분석 공격과 같은 부채널 공격에 강인하다는 장점을 지니고 있지만, RSA-CRT 연산 과정에서 특정 연산 부분에 공격자가 임의의 오류를 주입하는 경우 오동작이 발생하고 이때 출력된 연산의 결과를 이용하여 공격하려는 장치의 저장된 비밀 값 추출 가능하기 때문에 오류 주입 공격에 취약하다.

[5] 이러한 물리적 공격 중에서도 준침입성 공격에 해당하는 오류 주입 공격(Fault injection attack)은 침입성 공격과 같이 장치를 분해(Depackaging)한 후 오류를 주입해야 하는 공격이다.

[6] 구체적으로 칩의 패시베이션 층을 그대로 둔 채 직접적인 전기 접촉을 하지 않고 공격을 가하여 오류를 주입하는 것으로 X-ray나 전자기장, 혹은 레이저와 같은 빛을 이용하여 고의적인 오동작(Fault)을 일으키는 능동적인 공격이다.

[7] 특히, 이 공격의 경우 칩셋의 표면에서 정확한 위치를 찾아서 공격해야 하는 어려움이 있긴 하지만 비교적 용이하게 원하는 정보를 추출하는 하는 것이 가능하다.

[8] 이와 같은 오류 주입 공격에서도 레이저와 같은 광학적 오류를 주입하는 경우에는 공격하려는 칩의 내부 회로 중에서도 오류를 주입해야할 정확한 부분을 찾아서 디캡핑(decapping)하는 절차가 필요하다.

[9] 광학 오류 주입 공격은 도 1과 같이 암호화 알고리즘을 수행중인 마이크로 프로세서나 전용 암호화 칩에 레이저와 같은 빛을 주입하여 동작에 오류가 발생하게 함으로써 암호화에 필요한 비밀정보를 알아내는 공격이다.

[10] 암호화를 수행하는 칩의 패키지를 황산과 같은 용액을 이용해 제거하여 내부의 회로에 레이저와 같은 고에너지의 광선을 주입함으로써 오동작을 유발한다.

[11] 현재 많은 응용에서 표준으로 사용되고 있는 AES, RSA와 같은 표준 암호 알고리즘에 대한 다양한 광학 오류 주입 공격 기법이 소개되고 있으며, 방어책에 대한 연구도 활발히 진행 중이다.

[12] 이러한 광학 오류 주입을 방어하기 위한 기법은 크게 알고리즘 적인 방법과 물리적인 방법으로 나누어진다.

[13] 알고리즘 적인 방법 중 대표적인 방법은 알고리즘을 여러 번 수행하여 그 결과값을 비교하여 결과가 다를 경우 결과값을 출력하지 않는 방법이 있다. 혹은 암호화 알고리즘을 수행하는 블록을 여러 개를 배치하여 각각 다른 블록에서 수행된 결과값을 비교하는 방법이 있다. 그 외 특정 블록을 수행하기 이전에 계산된 체크섬 값과 수행한 이후의 체크섬 값을 비교하는 기법이 있다.

[14] 물리적인 방법으로는 칩의 탑 메탈(Top Metal)층 위에 금속판을 한 층 더 씌우는 메탈 쉴딩(Metal Shielding) 방법이 있다.

[15] 이 방법의 경우 레이저가 메탈층을 투과하지 못하도록 하여 공격을 방어하지만, 정교한 레이저를 이용하여 메탈층을 제거하는 것이 가능하며, 최근에는 칩의 바닥면인 실리콘(Silicon) 층을 통해 레이저를 주입하는 공격이 가능하므로 효과적인 해결책이 되지 못한다.

[16] 다른 방법으로는 DRL(Dual-Rail Logic) 기법이 있다.

[17] 이 기법은 1비트의 신호를 표현하기 위해 2비트를 이용하여 값을 엔코딩(encoding)하는 방법이다.

[18] 예를 들면, 0을 (0,1)로, 1을 (1,0)으로 표현하는 방법을 사용하여 모든 회로를 구성하며, 따라서 회로의 면적에 대한 비용이 2배 정도 발생한다.

[19] 이 방법을 이용하면, 상식적으로 발생할 수 없는 (1,1)의 상태를 광학 오류가 주입된 상태라고 정의하여 사용할 수 있다. 이는 (1,1)이라는 상태는 광학 오류 등으로 인해 회로 내에 조작이 없을 경우 발생할 수 없는 경우이기 때문이다.

[20] 또 다른 방법으로는 칩 내에 포토 다이오드(Photo Diode)와 같은 광센서를 장착하는 방법이다. 이는 광학 오류 주입을 위해 패키지가 제거되었을 경우 빛을 감지하기 위한 센서를 직접 칩에 장착하여 이러할 경우 칩을 동작시키지 못하도록 한다.

[21] 이 방법의 경우 포토 다이오드(Photo Diode)가 칩의 레이아웃에서 쉽게 발견될 수 있기 때문에, 해당 센서만을 마스킹 하는 방법이 가능하기 때문에 효과적이지 못하다.

[22] 이와 같은 칩 외부에서 오류 주입 공격에 의해 칩 내부의 비밀키와 같은 주요 정보가 노출되는 경우 해당 칩 및 이를 이용한 동종의 회로를 가지는 보안장치는 쉽게 보안이 해제되어 보호하고자 하는 대상을 보호할 수 없게 되는 문제점이 있다.

발명의 상세한 설명

기술적 과제

[23] 본 발명은 이와 같은 종래 기술의 오류 주입 공격에 대한 보호 방법의 문제를 해결하기 위한 것으로, 칩을 리셋하기 위해 필요한 리셋 신호선 상에 존재하는 버퍼들을 이용하여 광학 오류 주입을 감지할 수 있도록 한 리셋 신호 경로상의 버퍼를 이용한 광학 오류 주입 탐지 회로를 제공하는데 그 목적이 있다.

[24] 본 발명은 플립플롭의 리셋 포트로 연결되는 라우팅 경로 가운데에 있는 버퍼를 광학 오류 주입을 감지하는 센서로 사용하여 광학 오류 주입시 이를 탐지할 수 있도록 하여 광학 오류 주입 공격을 방어할 수 있도록 한 리셋 신호 경로상의 버퍼를 이용한 광학 오류 주입 탐지 회로를 제공하는데 그 목적이 있다.

[25] 본 발명의 목적들은 이상에서 언급한 목적들로 제한되지 않으며, 언급되지 않은 또 다른 목적들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제 해결 수단

[26] 이와 같은 목적을 달성하기 위한 본 발명에 따른 리셋 신호 경로상의 버퍼를 이용한 광학 오류 주입 탐지 회로는 디지탈 회로를 구성하는 각 플립플롭으로 전달되는 리셋 신호의 경로 상에 구성되어 외부의 광학 오류 주입을 감지하는 복수 개의 감지부;상기 감지부의 출력을 하나로 취합하여 어느 하나의 감지부의 신호에 변화가 발생하면 이를 구분하는 신호 취합부;상기 감지부에서 출력되는 신호 변화를 감지하여 신호 취합부의 입력에 의해 광학 오류 주입 탐지 신호를 발생시키는 탐지신호 발생부;를 포함하는 것을 특징으로 한다.

[27] 여기서, 상기 감지부는 디지탈 회로를 구성하는 각 플립플롭으로 전달되는 리셋 신호의 경로 상에 구성되는 버퍼 또는 인버터이고, 신호 취합부는 AND 게이트 또는 OR 게이트인 것을 특징으로 한다.

[28] 그리고 상기 광학 오류 주입을 감지하는 감지부로 사용되는 각 버퍼의 출력단에 플립플롭으로 탐지신호 발생부를 구성하고, 각각의 탐지신호 발생부의 출력을 취합하여 출력하는 신호 취합부로 OR 게이트를 사용하여 버퍼와 탐지신호 발생부의 거리가 최소화되도록 회로를 구성하는 것을 특징으로 한다.

[29] 그리고 상기 광학 오류 주입을 감지하는 감지부로 사용되는 각 버퍼의 출력을 취합하는 신호 취합부를 AND 게이트로 구성하고, 각각의 신호 취합부를 다단으로 구성하여 전단의 신호 취합부의 출력이 다음단의 신호 취합부로 입력되도록 회로를 구성하는 것을 특징으로 한다.

[30] 그리고 상기 광학 오류 주입을 감지하는 감지부로 사용되는 각 버퍼의 출력을 취합하는 신호 취합부를 다단으로 구성하여, 전단의 신호 취합부를 AND 게이트로 구성하여 출력이 탐지 신호 발생부로 입력되도록 하고, 탐지 신호

발생부의 출력이 입력되는 다음단의 신호 취합부를 OR 게이트로 구성하는 것을 특징으로 한다.

[31] 그리고 상기 디지탈 회로를 구성하는 각 플립플롭의 센싱 신호(sense_ff)는 클럭 신호(clock)의 하강 엣지(falling edge)에 값이 갱신되고, 초기에 리셋 신호로 인해 0인 값을 출력하다가 광학 오류 주입시 신호 취합부로 사용되는 AND 게이트의 출력이 0으로 변하기 때문에 이 시점에서 출력을 1로 갱신하여 광학 오류 주입이 있었음을 검출 신호(fault_detect)로 알리는 것을 특징으로 한다.

[32] 그리고 상기 감지부에 광학 오류가 주입될 경우 오류가 주입된 감지부의 출력이 뒤바뀌는 현상이 발생하며, 이는 각 감지부들의 출력 경로들을 통해 신호 취합부로 전달이 되며, 신호 취합부에서는 단 한 곳의 감지부라도 오류 주입을 탐지하면 이를 논리값 출력으로 구분하는 것을 특징으로 한다.

발명의 효과

[33] 이와 같은 본 발명에 따른 리셋 신호 경로상의 버퍼를 이용한 광학 오류 주입 탐지 회로는 다음과 같은 효과를 갖는다.

[34] 첫째, 광학 오류 주입 공격을 효율적으로 감지하여 효율적으로 오류 주입 공격에 대응할 수 있다.

[35] 둘째, 리셋 신호 경로상의 버퍼를 이용하여 광학 오류 주입을 탐지하므로 공격에 대한 방어를 위한 로직의 추가를 최소화할 수 있다.

[36] 셋째, 칩을 구성하기 위하여 반드시 필요하고, 이미 존재하는 리셋 신호 경로상의 버퍼를 이용하여 광학 오류 주입을 탐지하는 회로를 구성하므로 칩상에서의 면적 증가를 막고 제조 비용의 증가를 억제한다.

[37] 넷째, 리셋 신호 경로상의 버퍼를 이용하므로 버퍼에서 출력되는 신호를 취합하는 논리회로와 짧은 논리값 변화를 감지해 낼 수 있는 플립플롭 정도의 비용만으로 효과적으로 광학 오류 주입을 감지할 수 있다.

도면의 간단한 설명

[38] 도 1은 암호화 칩에 대한 광학 오류 주입 공격의 일 예를 나타낸 구성도

[39] 도 2는 본 발명에 따른 광학 오류 주입 탐지 회로의 기본 구성도

[40] 도 3은 본 발명에 따른 광학 오류 주입 탐지 회로의 상세 구성도

[41] 도 4 내지 도 6은 본 발명의 다른 실시 예에 따른 광학 오류 주입 탐지 회로의 구성도

[42] 도 7은 레이저 주입으로 인한 일시적인 전류 변화를 모델링한 버퍼 구성도

[43] 도 8은 본 발명에 따른 광학 오류 주입 탐지 회로에 대한 시뮬레이션 결과를 나타낸 그래프

[44] 도 9는 오류 주입 시점 확대를 나타낸 그래프

발명의 실시를 위한 최선의 형태

[45] 이하, 본 발명에 따른 리셋 신호 경로상의 버퍼를 이용한 광학 오류 주입 탐지 회로의 바람직한 실시 예에 관하여 상세히 설명하면 다음과 같다.

[46] 본 발명에 따른 리셋 신호 경로상의 버퍼를 이용한 광학 오류 주입 탐지 회로의 특징 및 이점들은 이하에서의 각 실시 예에 대한 상세한 설명을 통해 명백해질 것이다.

[47] 도 2는 본 발명에 따른 광학 오류 주입 탐지 회로의 기본 구성도이고, 도 3은 본 발명에 따른 광학 오류 주입 탐지 회로의 상세 구성도이다.

[48] 본 발명은 광학 오류 주입 공격을 효율적으로 감지하기 위한 방법으로 칩을 리셋하기 위해 필요한 리셋 신호선 상에 존재하는 버퍼들을 이용하여, 광학 오류 주입을 감지할 수 있도록 한 것이다.

[49] 일반적으로 하드웨어 칩에는 많은 수의 플립플롭을 사용하고 있으며, 이 플립플롭을 초기화하기 위해 리셋 신호가 사용되고 있는데, 이 신호는 칩 내부의 모든 플립플롭에 연결되어야 하기 때문에 칩의 전 영역에 거쳐 골고루 라우팅 되어야 한다.

[50] 또한, 많은 수의 플립플롭의 리셋 포트를 드라이브하기 위해서 라우팅 경로 중간에 많은 수의 버퍼가 추가되어 신호의 감소를 막는 역할을 한다.

[51] 본 발명에서는 이러한 플립플롭의 리셋 포트로 연결되는 라우팅 경로 가운데에 있는 버퍼를 광학 오류 주입을 감지하는 센서로 사용하는 것이다.

[52] 도 2에서와 같이 플립플롭의 CLK 포트와 RESET 포트를 모두 사용할 수 있으며 플립 플롭 대신에 LATCH를 사용하는 것도 가능하다.

[53] 도 3은 본 발명에서 제안하는 광학 오류 주입 탐지회로를 나타낸 것으로, ff0 ~ ff7의 플립플롭(121)(122)(123)은 디지털 회로에서 사용하는 일반적으로 사용되는 플립플롭이다.

[54] 리셋 신호의 경우 모든 플립플롭에 공급되어야 하는 신호이므로 High-fanout에 해당하는 신호이다. 모든 플립플롭에 리셋 신호가 잘 전달되기 위해서는 각 플립플롭의 리셋 포트를 드라이브할 수 있는 힘이 커야 하는데, 이를 위해 칩 내부에는 buffer1 ~ buffer4와 같은 버퍼(101)(102)(103)(104)가 삽입이 된다.

[55] 본 발명에서는 각 버퍼의 출력을 AND 게이트(131)로 묶어서 이를 광학 오류 주입 탐지 센서로 사용한다.

[56] 리셋 신호는 로우 액티브(low active) 이거나 하강 엣지(falling edge)를 감지하여 플립플롭을 초기화시키므로, 칩이 일반적인 동작을 할 경우 로직 1(high) 값을 가진다.

[57] 만약, 버퍼에 광학 오류가 주입이 되면, 광학 오류로 인해 발생한 에너지로 인해 로직 값이 0으로 변하게 되는데, 이를 감지하기 위해 탐지신호 발생을 위한 플립플롭(132)은 센싱 신호(sense_ff)가 필요하다.

[58] 센싱 신호(sense_ff)는 클럭 신호(clock)의 하강 엣지(falling edge)에 값이 갱신되는데, 초기에 리셋 신호로 인해 0인 값을 출력하다가, 광학 오류 주입시 AND 게이트의 출력이 0으로 변하기 때문에, 이 시점에서 출력을 1로 갱신하여 광학 오류 주입이 있었음을 검출 신호(fault_detect)로 알리게 된다.

[59] 이와 같은 본 발명에 따른 리셋 신호 경로상의 버퍼를 이용한 광학 오류 주입

탐지 회로의 기본 구성은 다음과 같다.

[60] 도 3에서와 같이, 디지털 회로(100)를 구성하는 플립플롭(121)(122)(123)과, 이 플립플롭(121)(122)(123)으로 전달되는 리셋 신호의 경로 상에 있는 감지부(101)(102)(103)(104)와, 감지부(101)(102)(103)(104)의 출력이 전달되는 경로(resetout0)(resetout1)(resetout7)를 거쳐 감지부(101)(102)(103)(104)에서 출력되는 신호를 취합하여 감지부(101)(102)(103)(104)중 한 곳에라도 광학 오류 주입이 감지될 경우 이를 구별하여 출력하는 신호취합부(131)와, 신호취합부(131)에서 출력되는 신호를 이용해 광학 오류가 발생하였음을 출력하는 탐지신호 발생부(132)로 구성된다.

[61] 이와 같이 구성되는 본 발명에 따른 리셋 신호 경로상의 버퍼를 이용한 광학 오류 주입 탐지 회로에서는 각 플립플롭(121)(122)(123)을 초기화하기 위한 목적으로 리셋 신호가 사용되며, High Fan-out 특성을 가지는 리셋 신호의 특성상 리셋 신호 경로 상에는 다수의 버퍼 즉 감지부(101)(102)(103)(104)가 장착된다.

[62] 이 버퍼(101)(102)(103)(104)에 광학 오류가 주입될 경우 오류가 주입된 버퍼의 출력이 뒤바뀌는 현상이 발생하며, 이는 버퍼의 출력 경로(resetout0)(resetout1)(resetout7)를 통해 신호 취합부(131)로 전달이 되며, 신호 취합부(131)에서는 단 한 곳의 감지부(101)(102)(103)(104)라도 오류 주입을 탐지하면 이를 논리값 출력으로 구분해 낼 수 있다.

[63] 탐지신호 발생부(132)는 광학 오류의 특성상 아주 짧은 시간 동안 발생하는 일시적인 논리값 변화를 잡아내어 이를 광학 오류를 탐지했다는 신호로 발생시켜주는 역할을 한다.

[64] 감지부(101)(102)(103)(104)에서 사용될 수 있는 버퍼는 기본적으로 짝수개의 인버터와 동일하기 때문에, 회로가 짝수개의 인버터를 통해 구현될 시에는 인버터도 감지부로 사용될 수 있으며, 리셋 신호가 전달되는 도선 역시 감지부가 될 수 있다.

[65] 신호 취합부(131)의 경우 AND 게이트를 사용하는 것으로 도시하였지만, 이는 하나의 예시에 불과하며, 여러 개의 감지부로부터의 신호를 취합하여 어느 하나의 감지부에서라도 광학 오류가 감지되었을 시 이를 구별해낼 수 있는 어떠한 형태의 논리 회로를 사용하는 것도 가능하다.

[66] 탐지신호 발생부(132) 역시 도 3에서는 플립플롭을 사용하는 것으로 설명하였으나, 플립플롭은 하나의 예에 불과하며, 짧은 시간에 발생하는 변화를 감지할 수 있는 어떠한 형태의 회로를 사용하여도 무방하다.

[67] 이와 같은 구성을 갖는 리셋 신호 경로상의 버퍼를 이용한 광학 오류 주입 탐지 회로를 다른 형태로 구성하는 경우에는 다음과 같다.

[68] 도 4 내지 도 6은 본 발명의 다른 실시 예에 따른 광학 오류 주입 탐지 회로의 구성도이다.

[69] 도 4는 본 발명에 따른 광학 오류 주입 탐지 회로의 다른 실시 예를 나타낸 것으로, 광학 오류 주입을 감지하는 감지부로 사용되는 여러 개의 버퍼를

통과하면서 오류 신호가 감쇄되어 광학 오류 주입을 탐지신호 발생부가 감지못하는 현상을 방지하기 위한 것이다.

[70] 즉, 광학 오류 주입을 감지하는 감지부로 사용되는 각 버퍼의 출력단에 탐지신호 발생부로 사용되는 플립 플롭을 구성하고, 각각의 탐지신호 발생부의 출력을 취합하여 출력하는 신호취합부로 OR 게이트를 사용하여 버퍼와 탐지신호 발생부의 거리가 최소화되도록 회로를 구성한 것이다.

[71] 도 5는 본 발명에 따른 광학 오류 주입 탐지 회로의 다른 실시 예를 나타낸 것으로, 광학 오류 주입을 감지하는 감지부로 사용되는 각 버퍼의 출력을 취합하는 신호 취합부를 AND 게이트로 구성하고, 각각의 신호 취합부를 다단으로 구성하여 전단의 신호 취합부의 출력이 다음단의 신호 취합부로 입력되도록 하여 광학 오류 주입 탐지의 정확성을 높인 것이다.

[72] 도 6은 본 발명에 따른 광학 오류 주입 탐지 회로의 다른 실시 예를 나타낸 것으로, 각각의 신호 취합부를 다단으로 구성하여 전단의 신호 취합부의 출력이 다음단의 신호 취합부로 입력되도록 하여 광학 오류 주입 탐지의 정확성을 높인 것으로, 탐지 신호 발생부를 전단의 신호 취합부의 출력단에 구성하여 탐지 신호 발생부의 출력이 OR 게이트로 구성되는 다음단의 신호 취합부의 입력이 되도록 한 것이다.

[73] 이와 같은 본 발명에 따른 리셋 신호 경로상의 버퍼를 이용한 광학 오류 주입 탐지 회로를 이용하여 광학 오류가 주입된 상황을 가정한 시뮬레이션을 수행하면 도 8에서와 같다.

[74] 도 7은 레이저 주입으로 인한 일시적인 전류 변화를 모델링한 버퍼 구성도이고, 도 8은 본 발명에 따른 광학 오류 주입 탐지 회로에 대한 시뮬레이션 결과를 나타낸 그래프이다.

[75] 그리고 도 9는 오류 주입 시점 확대를 나타낸 그래프이다.

[76] 도 7은 레이저 주입으로 인한 일시적인 전류 변화를 모델링한 버퍼 구성을 나타낸 것이다.

[77] 본 발명에 따른 광학 오류 주입 탐지 회로를 트랜지스터 레벨로 구성하여 SPICE 시뮬레이션을 수행한 결과는 도 8에서와 같다.

[78] 레이저가 CMOS의 pn 접합부에 주입이 될 경우 전자-양공의 형태로 흡수가 되며, 이로 인해 회로 상에 일시적인 전류 변화가 나타나게 되는데, 이때 발생하는 시간에 따른 전류량은 다음과 같은 수학식 1로 모델링 될 수 있다.

[79] 수학식 1

$$I(t) = I_0(e^{-t/\tau_\alpha} - e^{-t/\tau_\beta})$$

[80] 이 때, I(t)는 시간에 따른 전류 량이며, I_0는 전하로 인해 발생하는 최대 전류 값이며, τ_α는 접합에서의 전하 수집 시간 상수에 해당하며, τ_β는 이온 트랙(ion-track) 생성 시간 상수이다.

[81] 시뮬레이션을 위해서 오류가 주입되는 지점의 버퍼의 경우 수학식 1과 같은 형태로 일시적 전류가 발생하도록 도 7에서와 같이 전류 소스를 부착한다.

[82] 도 8은 광학 오류 주입 탐지 회로에 대한 시뮬레이션 결과를 나타낸 것으로, v()로 표시된 것은 전압을 나타내며, i()로 표시된 것은 전류량을 나타낸다.

[83] 25ns 부근에서 RESET 신호가 떨어지면 칩 내의 모든 플립플롭이 초기화된다.

[84] 이후 125ns에서 RESET 신호가 다시 올라가면 칩의 정상 동작이 시작된다.

[85] 225ns에서 모든 플립플롭의 입력으로 1(high)이 입력이 되는데 250ns에서 CLOCK의 rising edge에서 이값이 플립플롭에 반영이 되어 플립플롭의 출력 Q[0], Q[1]이 1(high) 값으로 변한다.

[86] 280ns에서 그림 3의 buffer2에 광학 오류가 주입이 되는데, 이로 인해 resetout0 출력이 일시적으로 떨어지며, Q[0] 출력이 0으로 바뀜을 확인할 수 있다. 이 오류 주입을 감지하여 fault_detect 출력이 1로 바뀜을 위의 파형에서 확인할 수 있다.

[87] 도 9는 오류가 주입된 시점을 확대한 것으로, resetout0의 전류량 변화는 ㅅ수학식1에서 제시된 것과 같이 double-exponent 형태로 변화하고 있음을 확인할 수 있으며, 이로 인한 resetout0의 전압 변화를 관찰할 수 있다.

[88] 이와 같은 본 발명에 따른 리셋 신호 경로상의 버퍼를 이용한 광학 오류 주입 탐지 회로는 플립플롭의 리셋 포트로 연결되는 라우팅 경로 가운데에 있는 버퍼를 광학 오류 주입을 감지하는 센서로 사용하여 광학 오류 주입시 이를 탐지할 수 있도록 하여 광학 오류 주입 공격을 방어할 수 있도록 한 것이다.

[89] 이상에서의 설명에서와 같이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 본 발명이 구현되어 있음을 이해할 수 있을 것이다.

[90] 그러므로 명시된 실시 예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 하고, 본 발명의 범위는 전술한 설명이 아니라 특허청구 범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

산업상 이용가능성

[91] 본 발명은 플립플롭의 리셋 포트로 연결되는 라우팅 경로 가운데에 있는 버퍼를 광학 오류 주입을 감지하는 센서로 사용하여 광학 오류 주입시 이를 탐지할 수 있도록 하여 광학 오류 주입 공격을 방어할 수 있도록 한 광학 오류 주입 탐지 회로를 제공하여 암호화 칩 제조 분야에 적용할 수 있다.

청구범위

[청구항 1] 디지탈 회로를 구성하는 각 플립플롭으로 전달되는 리셋 신호의 경로 상에 구성되어 외부의 광학 오류 주입을 감지하는 복수 개의 감지부;
상기 감지부의 출력을 하나로 취합하여 어느 하나의 감지부의 신호에 변화가 발생하면 이를 구분하는 신호 취합부;
상기 감지부에서 출력되는 신호 변화를 감지하여 신호 취합부의 입력에 의해 광학 오류 주입 탐지 신호를 발생시키는 탐지신호 발생부;를 포함하는 것을 특징으로 하는 리셋 신호 경로상의 버퍼를 이용한 광학 오류 주입 탐지 회로.

[청구항 2] 제 1 항에 있어서, 상기 감지부는 디지탈 회로를 구성하는 각 플립플롭으로 전달되는 리셋 신호의 경로 상에 구성되는 버퍼 또는 인버터인 것을 특징으로 하는 리셋 신호 경로상의 버퍼를 이용한 광학 오류 주입 탐지 회로.

[청구항 3] 제 1 항에 있어서, 상기 신호 취합부는 AND 게이트 또는 OR 게이트인 것을 특징으로 하는 리셋 신호 경로상의 버퍼를 이용한 광학 오류 주입 탐지 회로.

[청구항 4] 제 1 항에 있어서, 상기 광학 오류 주입을 감지하는 감지부로 사용되는 각 버퍼의 출력단에 플립플롭으로 탐지신호 발생부를 구성하고,
각각의 탐지신호 발생부의 출력을 취합하여 출력하는 신호 취합부로 OR 게이트를 사용하여 버퍼와 탐지신호 발생부의 거리가 최소화되도록 회로를 구성하는 것을 특징으로 하는 리셋 신호 경로상의 버퍼를 이용한 광학 오류 주입 탐지 회로.

[청구항 5] 제 1 항에 있어서, 상기 광학 오류 주입을 감지하는 감지부로 사용되는 각 버퍼의 출력을 취합하는 신호 취합부를 AND 게이트로 구성하고,
각각의 신호 취합부를 다단으로 구성하여 전단의 신호 취합부의 출력이 다음단의 신호 취합부로 입력되도록 회로를 구성하는 것을 특징으로 하는 리셋 신호 경로상의 버퍼를 이용한 광학 오류 주입 탐지 회로.

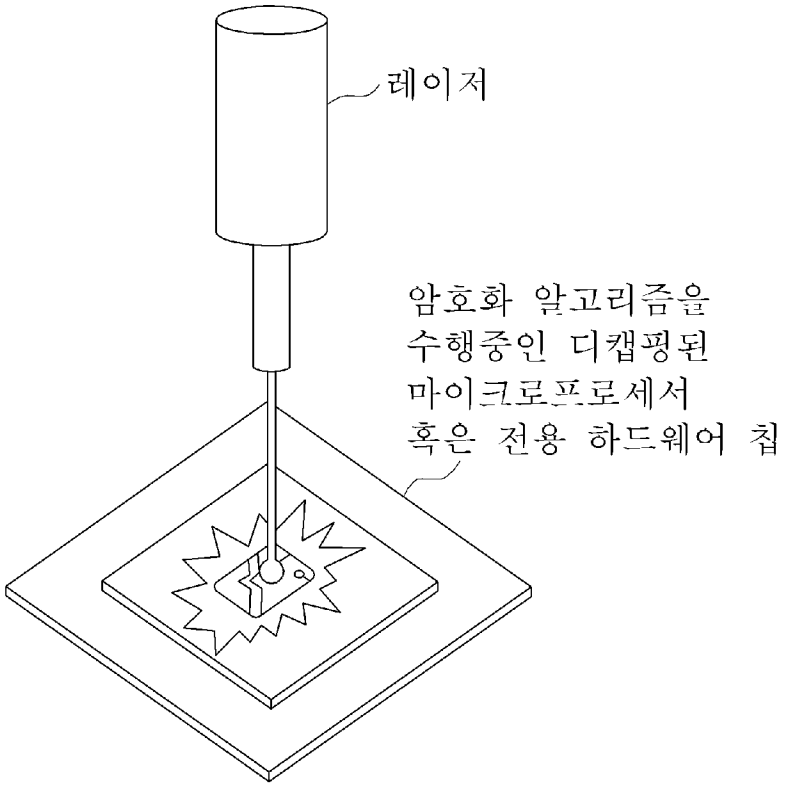
[청구항 6] 제 1 항에 있어서, 상기 광학 오류 주입을 감지하는 감지부로 사용되는 각 버퍼의 출력을 취합하는 신호 취합부를 다단으로 구성하여,
전단의 신호 취합부를 AND 게이트로 구성하여 출력이 탐지 신호 발생부로 입력되도록 하고, 탐지 신호 발생부의 출력이 입력되는 다음단의 신호 취합부를 OR 게이트로 구성하는 것을 특징으로

하는 리셋 신호 경로상의 버퍼를 이용한 광학 오류 주입 탐지 회로.

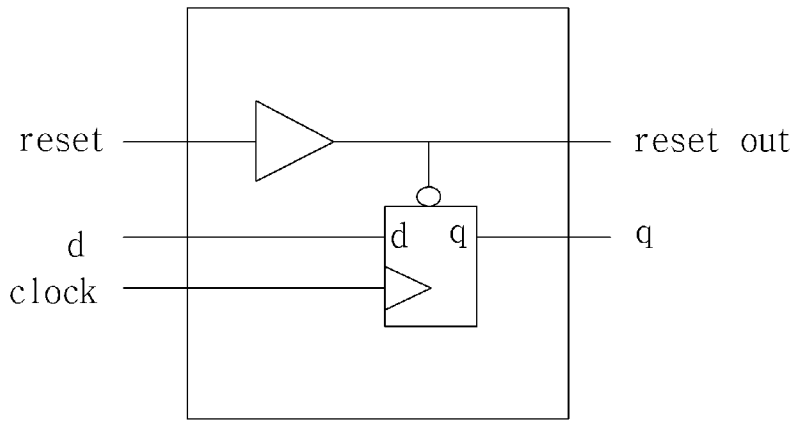
[청구항 7] 제 1 항에 있어서, 상기 디지탈 회로를 구성하는 각 플립플롭의 센싱 신호(sense_ff)는 클럭 신호(clock)의 하강 엣지(falling edge)에 값이 갱신되고, 초기에 리셋 신호로 인해 0인 값을 출력하다가 광학 오류 주입시 신호 취합부로 사용되는 AND 게이트의 출력이 0으로 변하기 때문에 이 시점에서 출력을 1로 갱신하여 광학 오류 주입이 있었음을 검출 신호(fault_detect)로 알리는 것을 특징으로 하는 리셋 신호 경로상의 버퍼를 이용한 광학 오류 주입 탐지 회로.

[청구항 8] 제 1 항에 있어서, 상기 감지부에 광학 오류가 주입될 경우 오류가 주입된 감지부의 출력이 뒤바뀌는 현상이 발생하며, 이는 각 감지부들의 출력 경로들을 통해 신호 취합부로 전달이 되며, 신호 취합부에서는 단 한 곳의 감지부라도 오류 주입을 탐지하면 이를 논리값 출력으로 구분하는 것을 특징으로 하는 리셋 신호 경로상의 버퍼를 이용한 광학 오류 주입 탐지 회로.

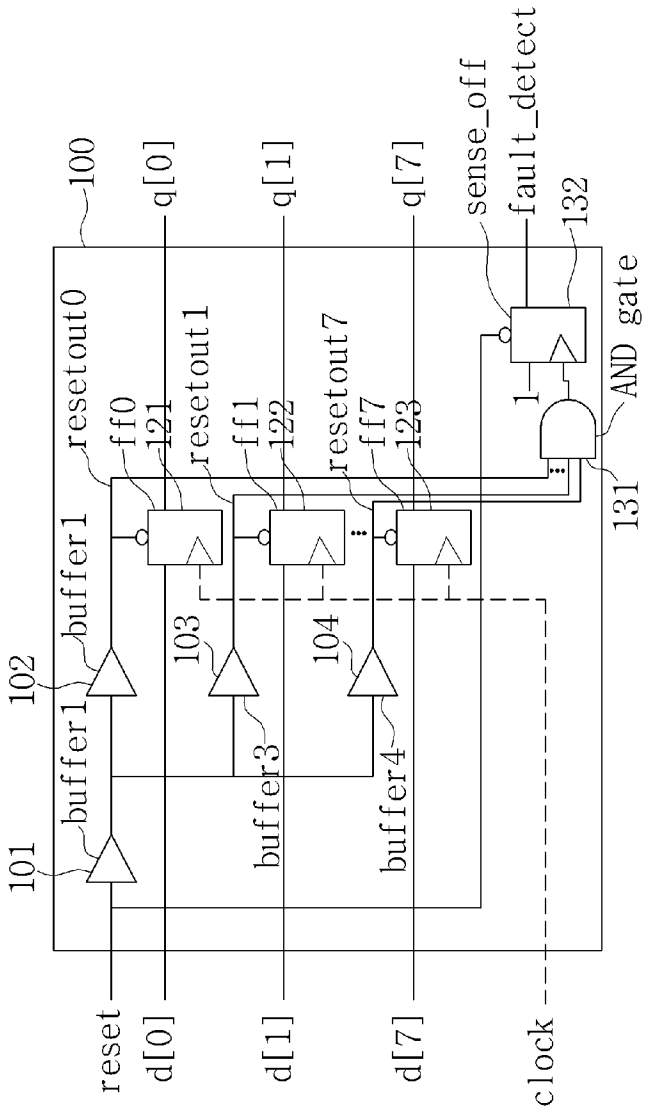
[Fig. 1]


레이저
암호화 알고리즘을
수행중인 디캡핑된
마이크로프로세서
혹은 전용 하드웨어 칩

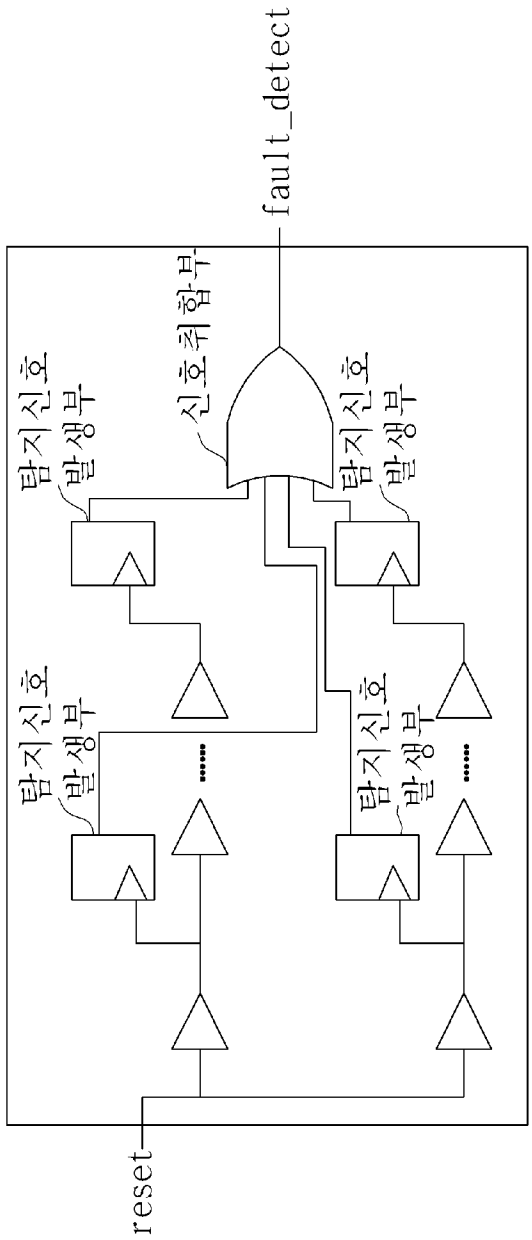
[Fig. 2]


reset
reset out
d
d q
q
clock

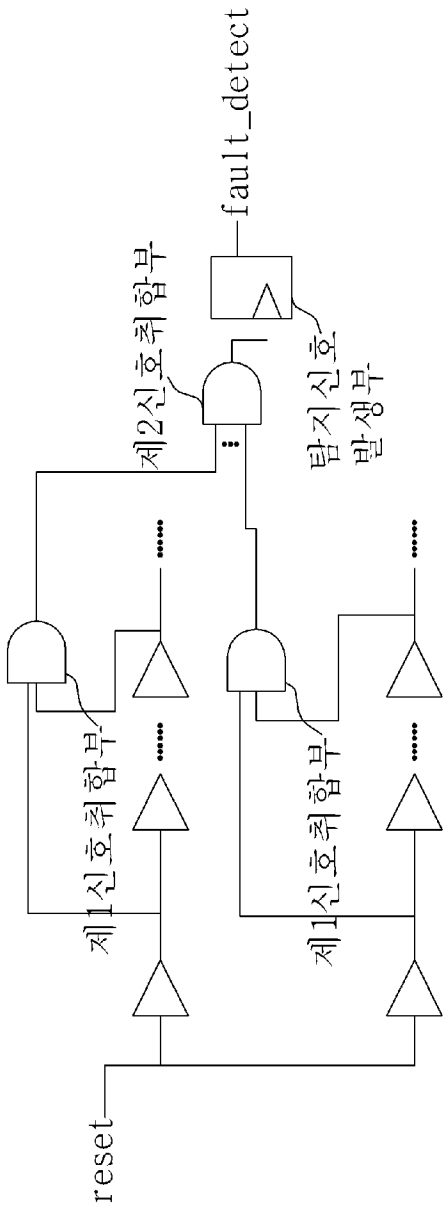
[Fig. 3]


100
q[0]
q[1]
q[7]
sense_off
fault_detect
132
resetout0
ff0
121
resetout1
ff1
122
resetout7
ff7
123
1
AND gate
131
buffer1
102
buffer1
101
103
104
buffer3
buffer4
reset
d[0]
d[1]
d[7]
clock

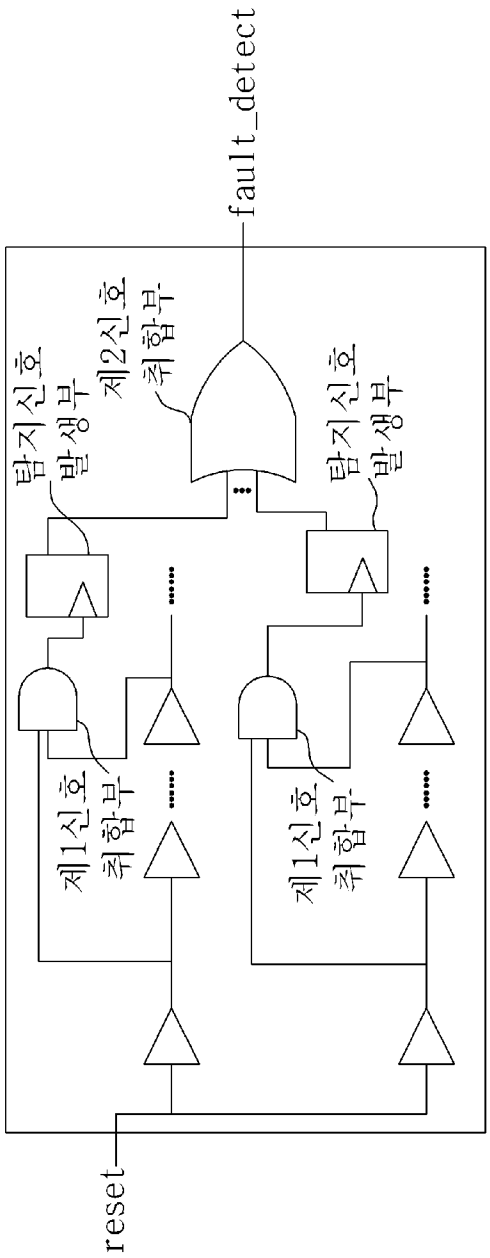
[Fig. 4]



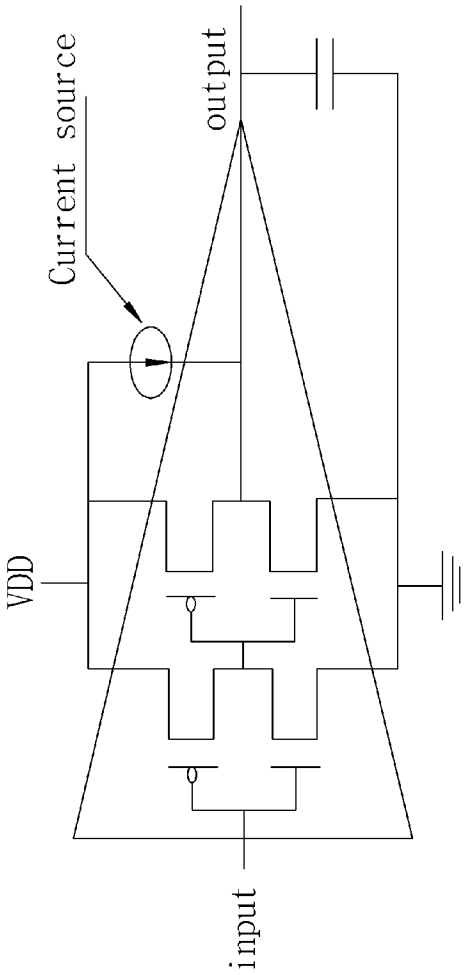
[Fig. 5]



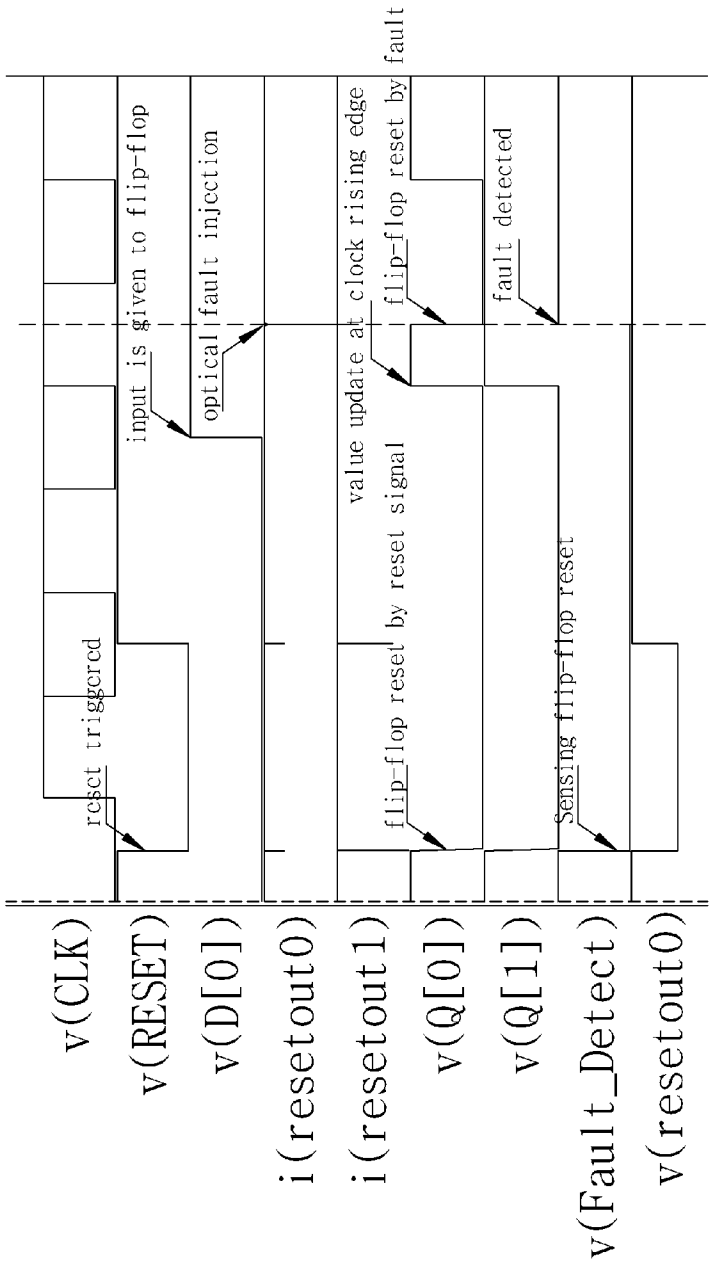
[Fig. 6]


fault_detect
탐지신호 발생부
제2신호 취합부
탐지신호 발생부
제1신호 취합부
제1신호 취합부
reset

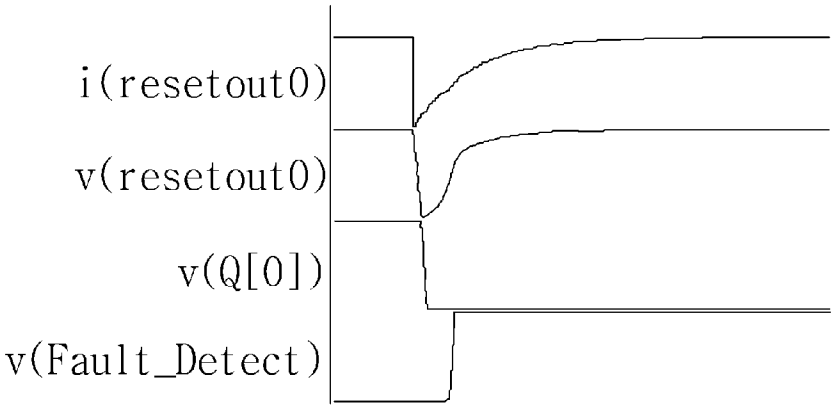
[Fig. 7]



[Fig. 8]


reset triggered
input is given to flip-flop
optical fault injection
value update at clock rising edge
flip-flop reset by reset signal
flip-flop reset by fault
fault detected
Sensing flip-flop reset
v(CLK)
v(RESET)
v(D[0])
i(resetout0)
i(resetout1)
v(Q[0])
v(Q[1])
v(Fault_Detect)
v(resetout0)

[Fig. 9]


i(resetout0)
v(resetout0)
v(Q[0])
v(Fault_Detect)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2013/008109

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/861(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L 12/861; G06F 11/34; G06K 19/07; H03K 3/356; H04B 10/07; G06F 21/06; H04B 10/25; G05B 23/02; H03K 3/037

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean Utility models and applications for Utility models: IPC as above
Japanese Utility models and applications for Utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: optical fault injection, detection circuit, reset signal path, buffer, flip-flop

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KR 10-2009-0111724 A (LIG NEOPTEK CO.,LTD) 27 October 2009 See abstract, claims 1, 2 and figures 2-8	1-8
A	JP 2009-259126 A (DAINIPPON PRINTING CO., LTD.) 05 November 2009 See abstract, claims 4-6 and figures 1-7	1-8
A	US 2011-0119532 A1 (TEGLIA, Yannick) 19 May 2011 See abstract, claim 1 and figures 1-5	1-8
A	KR 10-2010-0065708 A (UNIVERSITY-INDUSTRY COOPERATION GROUP OF KYUNG HEE UNIVERSITY) 17 June 2010 See abstract, claims 1-3 and figures 4-13	1-8
A	KR 10-0296984 B1 (NISSAN MOTOR CO., LTD.) 24 October 2001 See claims 1-3 and figures 3-8	1-8

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 DECEMBER 2013 (16.12.2013)	**17 DECEMBER 2013 (17.12.2013)**
Name and mailing address of the ISA/KR Korean Intellectual Property Office Government Complex-Daejeon, 189 Seonsa-ro, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2013/008109

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2009-0111724 A	27/10/2009	NONE	
JP 2009-259126 A	05/11/2009	NONE	
US 2011-0119532 A1	19/05/2011	EP 2326042 A1 EP 2326042 B1	25/05/2011 03/04/2013
KR 10-2010-0065708 A	17/06/2010	NONE	
KR 10-0296984 B1	24/10/2001	JP 03520662 B2 JP 09-282024 A US 6076172 A	19/04/2004 31/10/1997 13/06/2000

국 제 조 사 보 고 서

국제출원번호
PCT/KR2013/008109

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04L 12/861(2013.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

H04L 12/861; G06F 11/34; G06K 19/07; H03K 3/356; H04B 10/07; G06F 21/06; H04B 10/25; G05B 23/02; H03K 3/037

조사된 기술분야에 속하는 최소문헌 이외의 문헌

한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC
일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))

eKOMPASS(특허청 내부 검색시스템) & 키워드:광학 오류 주입, 탐지 회로, 리셋 신호 경로, 버퍼, 플립플롭

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	KR 10-2009-0111724 A (엘아이지네옵텍 주식회사) 2009.10.27 요약, 청구항 1, 2 및 도면 2-8 참조	1-8
A	JP 2009-259126 A (DAINIPPON PRINTING CO., LTD.) 2009.11.05 요약, 청구항 4-6 및 도면 1-7 참조	1-8
A	US 2011-0119532 A1 (YANNICK TEGLIA) 2011.05.19 요약, 청구항 1 및 도면 1-5 참조	1-8
A	KR 10-2010-0065708 A (경희대학교 산학협력단) 2010.06.17 요약, 청구항 1-3 및 도면 4-13 참조	1-8
A	KR 10-0296984 B1 (닛산 지도샤 가부시키가이샤) 2001.10.24 청구항 1-3 및 도면 3-8 참조	1-8

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

"A" 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

"E" 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

"L" 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

"O" 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

"T" 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

"X" 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

"Y" 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2013년 12월 16일 (16.12.2013)	2013년 12월 17일 (17.12.2013)

ISA/KR의 명칭 및 우편주소
대한민국 특허청
(302-701) 대전광역시 서구 청사로 189, 4동 (둔산동, 정부대전청사)
팩스 번호 +82-42-472-7140

심사관
이동윤
전화번호 +82-42-481-8734

국제조사보고서
대응특허에 관한 정보

국제출원번호
PCT/KR2013/008109

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2009-0111724 A	2009/10/27	없음	
JP 2009-259126 A	2009/11/05	없음	
US 2011-0119532 A1	2011/05/19	EP 2326042 A1 EP 2326042 B1	2011/05/25 2013/04/03
KR 10-2010-0065708 A	2010/06/17	없음	
KR 10-0296984 B1	2001/10/24	JP 03520662 B2 JP 09-282024 A US 6076172 A	2004/04/19 1997/10/31 2000/06/13