



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2013-0047401
(43) 공개일자 2013년05월08일

(51) 국제특허분류(Int. Cl.)
H03K 19/20 (2006.01) G06F 7/00 (2006.01)
(21) 출원번호 10-2011-0112402
(22) 출원일자 2011년10월31일
심사청구일자 2011년10월31일

(71) 출원인
동서대학교산학협력단
부산광역시 사상구 주례동 산 69-1 동서대학교
(72) 발명자
박영구
경남 창원시 반림동 럭키아파트 41동 1102호
이훈재
대구광역시 동구 신암4동 SD 아이프라임 102-707
황기현
부산광역시 해운대구 반여동 아시아선수촌아파트
115동 1205호
(74) 대리인
김일환

전체 청구항 수 : 총 3 항

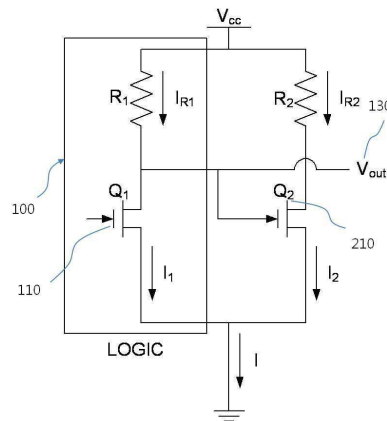
(54) 발명의 명칭 해밍 웨이트 모델을 이용한 전력 분석공격 방지 논리회로 및 이를 포함하는 스마트 카드

(57) 요약

본 발명은 해밍 웨이트 모델을 이용한 전력 분석공격 방지 논리회로 및 이를 포함한 스마트 카드에 관한 것으로, 논리 게이트를 포함하는 논리 회로와, 상기 논리 게이트의 출력단에 상기 논리 게이트와 동일한 특성의 FET 소자가 설치되어, 상기 논리 회로의 전체 전류를 일정하게 유지시키는 것을 특징으로 한다.

이와 같은 본 발명은, 논리회로에 간단한 소자의 설치와 구성으로, 암호화 프로세스를 수행하는 논리회로의 출력단에서 전력신호 또는 전류신호를 측정하더라도 일정한 값을 도출시켜 전력 분석공격을 원천적으로 차단할 수 있는 전력 분석공격 방지 논리회로를 제공할 수 있게 된다.

대표도 - 도1



특허청구의 범위

청구항 1

논리 게이트를 포함하는 논리 회로와,

상기 논리 게이트의 출력단에 상기 논리 게이트와 동일한 특성의 FET 소자가 설치되어,

상기 논리 회로의 전체 전류를 일정하게 유지시키는 것을 특징으로 하는 해밍 웨이트 모델을 이용한 전력 분석 공격 방지 논리회로.

청구항 2

MOS형의 논리 게이트 회로와,

상기 논리 게이트 회로의 출력단에 설치되는 FET 소자와,

상기 논리 게이트 입력단에 설치되는 가변저항을 포함하되,

상기 가변저항의 조정을 통해 논리 회로 전체 전류를 일정하게 유지시키는 것을 특징으로 하는 해밍 웨이트 모델을 이용한 전력 분석공격 방지 논리회로.

청구항 3

제1항 또는 제3항 중 어느 한 항의 전력 분석공격 방지 논리회로를 포함하는 스마트 카드.

명세서

기술분야

- [0001] 본 발명은 전력 분석공격 방지 논리회로에 관한 것으로, 보다 상세하게는 간단한 구성으로 해밍 웨이트 모델을 이용한 전력 분석공격을 방지할 수 있는 논리회로 및 이를 포함하는 스마트 카드에 관한 것이다.

배경기술

- [0002] 스마트 카드는 마이크로 프로세서와 메모리를 통한 데이터 연산 처리 기능과 데이터 저장 기능을 바탕으로 1990년 이후 본격적으로 전자상거래, 이동 통신, 금융 결제, 교통, 의료 등 다양한 응용 분야에 사용되고 있다. 이와 같은 스마트 카드의 이용 분야가 급격히 확대되어 감에 따라 고도의 보안성과 안전성이 필요하게 되었다.
- [0003] 암호학자들은 기존의 수학기론들을 배경으로 가능한 수학적 공격방법들에 대해 안전할 수 있는 알고리즘들을 개발해 왔다. 하지만 암호시스템의 구현 시 암호알고리즘의 설계에 고려되지 못한 비밀정보의 누출을 발생시킬 수 있다. 특히 스마트 카드의 구현 시 비밀키에 대한 연산이 빈번히 일어남으로 이 비밀정보의 누출이 시스템의 안전도에 큰 영향을 끼칠 수 있다.
- [0004] 전력분석 공격은 Crypto' 99에서 Paul Kocher에 의해 DES에 적용시킴으로서 제안된 방법으로, 만약 공격자가 스마트 카드 비밀키의 일부 Hamming weight를 알고 있다면 전탐색(brute force search)의 가능한 키 영역을 줄일 수 있고 충분한 hamming weight가 주어진다면 전체 비밀키에 대한 정보를 알 수 있다.
- [0005] 이와 같은 전력분석 공격은 크게 스마트 카드 내부의 비밀키의 연산시 직접 소비전력신호의 특성을 파악하여 비밀키에 대한 정보를 알아내는 SPA(Simple Power Analysis)와 SPA에 통계적인 분석방법과 여러 정정 기술을 첨가한 DPA(Differential power analysis), 그리고 IPA(Inferential power analysis)로 나누어 질 수 있다.
- [0006] 일반적으로 전력분석 공격은 일반 게이트 소자에 출력신호가 "0"일때와 "1"일 때 결과 값의 변환순간에 외부에서 전력변환 상태를 검출가능하기 때문에 상술한 하드웨어적인 해킹(DPA)이 가능하였다. 따라서 보안대책에서는

이들 변화를 외부에서 파형 검출할 수 없도록 해야 하는 문제점이 있다.

발명의 내용

해결하려는 과제

- [0007] 상술한 문제를 해결하고자 하는 본 발명의 과제는 논리회로에 간단한 소자의 설치와 구성으로, 암호화 프로세스를 수행하는 논리회로의 출력단에서 전력신호 또는 전류신호를 측정하더라도 일정한 값을 도출시켜 전력 분석공격을 원천적으로 차단할 수 있는 전력 분석공격 방지 논리회로 및 보안 기능이 강화된 스마트 카드를 제공하고자 함이다.

과제의 해결 수단

- [0008] 상술한 문제를 해결하는 본 발명의 제1 특징은 논리 게이트를 포함하는 논리 회로와, 상기 논리 게이트의 출력단에 상기 논리 게이트와 동일한 특성의 FET 소자가 설치되어, 상기 논리 회로의 전체 전류를 일정하게 유지시키는 것이다.
- [0009] 또한, MOS형의 논리 게이트 회로와, 상기 게이트 회로의 출력단에 설치되는 FET 소자와, 상기 논리 게이트 입력단에 설치되는 가변저항을 포함하되, 상기 가변저항의 조정을 통해 논리 회로 전체 전류를 일정하게 유지시키는 것을 특징으로 한다.
- [0010] 그리고, 본 발명의 제2 특징은 상술한 전력 분석공격 방지 논리회로를 포함하는 스마트 카드를 제안하는 것이다.

발명의 효과

- [0011] 이와 같은 본 발명은, 논리회로에 간단한 소자의 설치와 구성으로, 암호화 프로세스를 수행하는 논리회로의 출력단에서 전력신호 또는 전류신호를 측정하더라도 일정한 값을 도출시켜 전력 분석공격을 원천적으로 차단할 수 있는 전력 분석공격 방지 논리회로를 제공할 수 있게 된다.
- [0012] 또한, 상술한 해밍 웨이트 모델을 이용한 전력 분석공격 방지 논리회로를 포함하는 스마트 카드를 제공함으로써 간단한 구성으로 보안 기능을 강화시킬 수 있게 된다.

도면의 간단한 설명

- [0013] 도 1은 본 발명에 따른 해밍 웨이트 모델을 이용한 전력 분석공격 방지 논리회로의 구성을 나타낸 회로도,
 도 2는 본 발명에 따른 전력 분석공격 방지 논리회로의 효과를 비교하기 위한 인버트 게이트 회로의 구성(도 2의 (a))과 그 전체 전류의 변화 그래프(도 2의 (b))를 나타낸 도면,
 도 3은 본 발명에 따른 또 다른 실시예로서, 해밍 웨이트 모델을 이용한 전력 분석공격 방지 논리회로의 구성을 나타낸 회로도(도 3의 (a)), 출력단 전압 또는 전류의 그래프,
 도 4는 본 발명에 따른 또 다른 실시예로서, 해밍 웨이트 모델을 이용한 전력 분석공격 방지 논리회로의 구성을 나타낸 회로도이다.

발명을 실시하기 위한 구체적인 내용

- [0014] 본 발명의 이점 및 특징, 그리고 그것을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 통해 설명될 것이다. 그러나 본 발명은 여기에서 설명되는 실시예들에 한정되지 않고 다른 형태로 구체화될 수도 있다. 단지, 본 실시예들은 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 본 발명의 기술적 사상을 용이하게 실시할 수 있을 정도로 상세히 설명하기 위하여 제공되는 것이다.
- [0015] 도면들에 있어서, 본 발명의 실시예들은 도시된 특정 형태로 제한되는 것이 아니며 명확성을 기하기 위하여 과장된 것이다. 또한 명세서 전체에 걸쳐서 동일한 참조번호로 표시된 부분들은 동일한 구성요소를 나타낸다.
- [0016] 본 명세서에서 "및/또는"이란 표현은 전후에 나열된 구성요소들 중 적어도 하나를 포함하는 의미로 사용된다. 또한, 단수형은 문구에서 특별히 언급하지 않는 한 복수형도 포함한다. 또한, 명세서에서 사용되는 "포함한다"

또는 "포함하는"으로 언급된 구성요소, 단계, 동작 및 소자는 하나 이상의 다른 구성요소, 단계, 동작, 소자 및 장치의 존재 또는 추가를 의미한다.

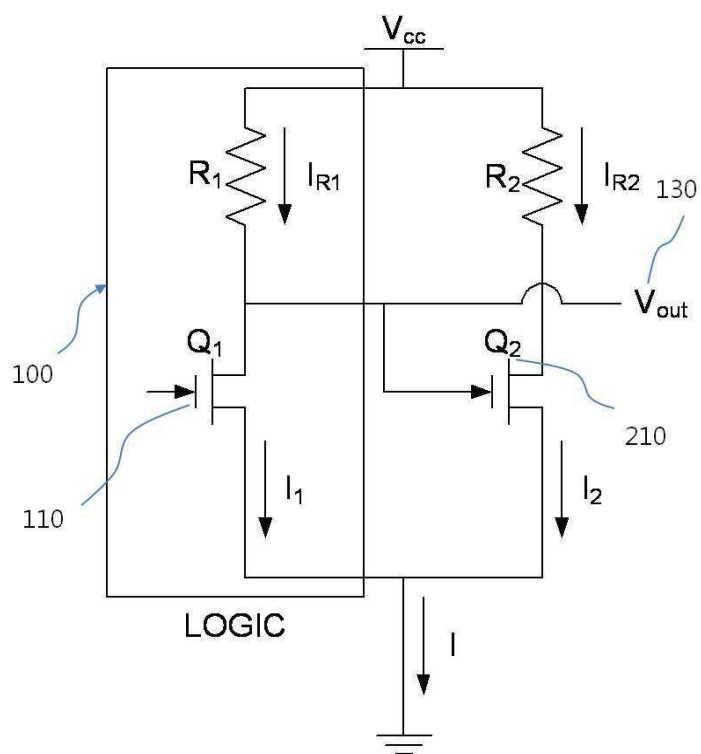
- [0017] 이하에서 본 발명에 따른 바람직한 실시예를 도면을 참조하여 상세히 설명하기로 한다.
- [0018] 도 1은 본 발명에 따른 해밍 웨이트 모델을 이용한 전력 분석공격 방지 논리회로의 구성을 나타낸 회로도이다. 도 1에 나타낸 바와 같이, 본 발명의 실시예에 따른 전력 분석공격 방지 논리회로는 논리 게이트(110)를 포함하는 논리 회로(100)와, 상기 논리 게이트(110)의 출력단(130)에 상기 논리 게이트(110)와 동일한 특성의 FET 소자(210)가 설치되어, 상기 논리 회로의 전체 전류를 일정하게 유지시키는 것을 특징으로 한다.
- [0019] 일반적으로 스마트 카드 등의 해킹을 위한 전력 분석공격은 SPA(simple power analysis) 및 DPA(differential power analysis)로 분류된다. SPA 공격은 스마트 카드에서 연산되는 암호 프로세서의 전력소비를 직접 관찰하여 카드내부에 저장되어 있는 비밀키를 알 수 있는 공격방법이다. 실제로, 스마트 카드 내에서 소비되는 전력을 측정하기 위해서는 스마트 카드의 접지 부분과 전력 공급기의 접지사이에 10 ~ 50 Ω 정도의 작은 값을 갖는 저항을 직렬로 연결하여 소비되는 전력을 측정할 수 있다.
- [0020] 스마트 카드내의 암호 프로세서는 수행되어 지는 명령(instruction)에 따라 저마다 서로 다른 소비 전력 신호 특성을 가지므로, 공격자는 상기 소비 전력 신호 특성을 나타내는 정보를 이용하여 스마트 카드 내부의 비밀키에 따라 수행되는 명령의 특성을 파악하여 그 명령의 순서를 역추적 함으로써 내부 비밀키를 알아낸다.
- [0021] DPA 공격은 SPA 공격보다 방어하기 더 어려운 강력한 공격방법으로 기존의 SPA의 소비 전력 관찰하는 것에 더하여 비밀키와 정확히 상관 관계(correlation)를 가지는 정보를 추출하기 위해 통계적인 분석(statistical analysis)과 에러 정정(error correction) 기술을 사용한다.
- [0022] 이와 같은 전력 분석공격 방법에 대하여 공격을 방지하기 위해서 본 발명에서는 도 1에 나타낸 바와 같이, 논리 게이트(110)의 출력단(130)에 FET 소자(210)를 설치하여, 암호화 프로세스를 위한 논리 회로의 동작에 의한 전력 신호를(전체 전류) 일정하게 유지시키도록 하여 원천적으로 전력분석 공격을 방지하기 위한 논리회로 구성을 제안한다.
- [0023] 도 1을 참조하면, 하나의 FET 소자(210)의 저항(R_1)으로 이루어진 논리 게이트에서, V_{out} 즉 논리 게이트 출력은 H/L이라고 할때, 출력단의 전압은 $V_{out} = H$ 로서, FET 소자에서 Q_1 에 인가되는 전압이 0인 경우, 즉, $Q_1 = OFF$ 경우, $i_1 = 0$, $Q_2 = ON$ 이므로 $i_2 = IR_2$ 가 된다. 그러므로 전체 전류는 $i = i_2 = IR_2$ 가 된다.
- [0024] $V_{out} = L$ 로서, 논리 게이트 회로의 FET 소자의 $Q_1 = ON$ 인 경우, $i_1 = IR_1$ 이고, $Q_2 = OFF$ 인 경우 $i_2 = 0$ 이 된다. 그러므로 논리 회로의 전체 전류는 $i = i_1 = IR_1$ 이 된다.
- [0025] 이와 같이 Q_1 과 Q_2 에 교대로 전원이 인가되는 경우에, 서로 다른 전체 전류가 나타나지만, R_1 과 R_2 를 동일한 저항값으로 사용하는 경우 상술한 바와 같이, $i = IR_1 = IR_2$ 로 같아져서, 외부의 장치를 통해 변화되는 전력 또는 전류신호를 파악할 수 없게 되기 때문에, 전력 분석공격을 수행할 수 없게 된다.
- [0026] 즉, 본 발명에 따른 실시예로서, 해밍 웨이트 모델을 이용한 전력 분석공격 방지 논리회로는 논리 게이트 회로의 출력단에 동일한 특성을 갖는 FET 소자를 설치하고, 저항값을 조정하게 되면, 암호화 프로세스를 수행하는 논리회로의 출력단에서 전력신호 또는 전류신호를 측정하더라도 일정한 값을 도출시키기 때문에 전력 분석공격을 원천적으로 차단할 수 있는 효과를 얻을 수 있다.
- [0027] 도 2는 본 발명에 따른 전력 분석공격 방지 논리회로의 효과를 비교하기 위한 인버트 게이트 회로의 구성(도 2의 (a))과 그 전체 전류의 변화 그래프(도 2의 (b))를 나타낸 도면이다.
- [0028] 도 2에 나타낸 바와 같이, 인버트 게이트 회로의 입력단 전압 V_{in} 0V 인 경우, Q_1 은 ON, Q_2 는 OFF가 되며, 출력 전압 V_{out} 은 V_{cc} 가 되고, 전체 전류 I 는 0이 된다. 그리고, 입력단 전압 V_{in} 이 5V 인 경우, Q_1 은 OFF, Q_2 는 ON이

되며, 출력 전압 V_{out} 은 0이 되고, 전체 전류 I 는 I_1 가 된다.

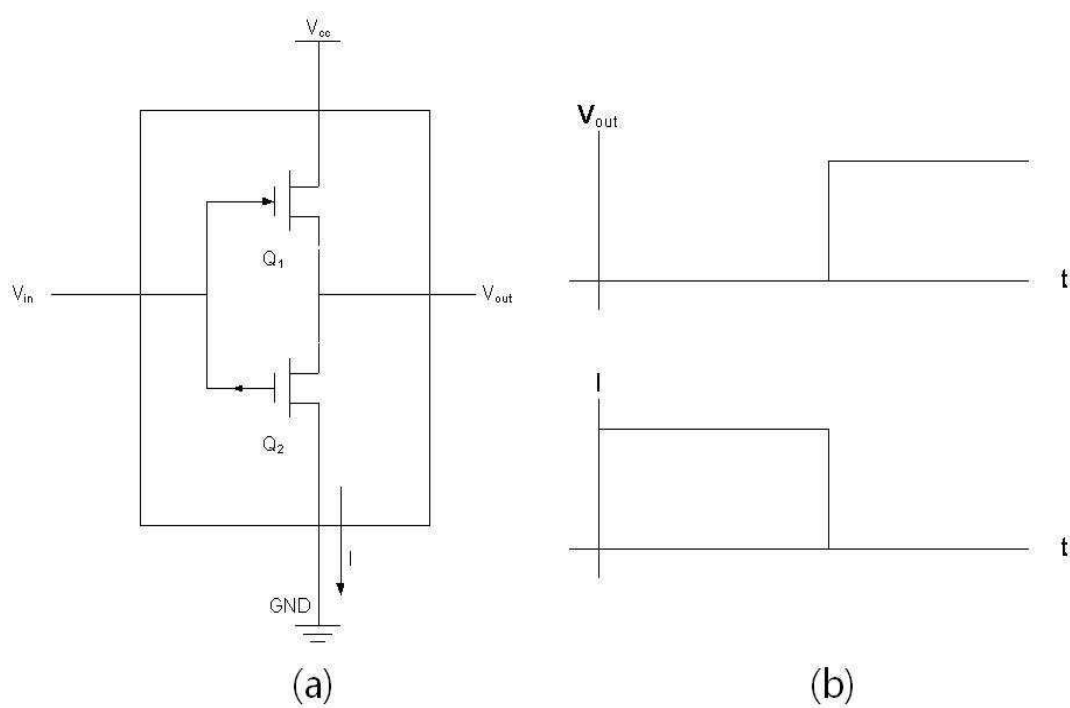
- [0029] 상술한 논리 회로의 신호에 대한 출력된 전류 또는 전압의 결과는 도 2의 (b)에 나타난 바와 같이, 입력단 신호의 변화가 있을 때마다, 출력단의 전류 또는 전압의 결과도 같이 변화기 때문에, 전력분석 공격으로 용이하게 해킹할 수 있는 문제점이 있었다.
- [0030] 이와 같은 이유로, 본 발명에서는 논리 게이트의 출력단에 논리 게이트와 특성이 동일한 FET 회로를 추가하여, 논리 게이트의 출력 전류 또는 전압의 변화에 무관하게 논리 게이트의 전체 전류량을 일정하게 유지하므로, 해밍 웨이트 모델(Hamming Weight Model)을 이용한 DPA에 의한 방어 기능을 제공하는 회로를 제안한다.
- [0031] 여기서, 해밍 웨이트 모델(Hamming Weight Model)을 이용한 DPA 공격은 스마트 카드내의 프로세서는 데이터가 처리되어 지는 과정에서 데이터의 해밍 웨이트(hamming weight)의 값을 갖는 데이터는 낮은 해밍 웨이트의 값을 갖는 데이터보다 데이터 처리과정에서 더 많은 전력을 소비하기 때문에, 비밀키와 메시지가 연산될 때 소비되는 전력을 이용하여 비밀키를 알아내는 방법을 말한다.
- [0032] 그러므로, 본 발명에서는 프로세서 즉, 논리 게이트 회로의 출력단에 동일한 특성의 FET 소자를 설치하여 출력단의 전류의 값을 일정하게 함으로써, 해밍 웨이트(hamming weight) 값을 거의 같게 하여 비밀키와 메시지가 연산될 때 소비되는 전력을 이용한 비밀키를 알아내는 것을 원천적으로 봉쇄하는 것을 제안한다.
- [0033] 도 3은 본 발명에 따른 또 다른 실시예로서, 해밍 웨이트 모델을 이용한 전력 분석공격 방지 논리회로의 구성을 나타낸 회로도(도 3의 (a)), 출력단 전압 또는 전류의 그래프이다.(도 3의 (b))
- [0034] 도 3에 나타난 바와 같이, 본 발명의 실시예에 따른 전력 분석공격 방지 논리회로는 2개의 FET 소자로 이루어진 논리 게이트 회로(111)와, 상기 논리 게이트의 출력단에 상기 논리 게이트와 동일한 특성의 FET 소자(210)가 설치되어, 상기 논리 회로의 전체 전류를 일정하게 유지시키는 것을 특징으로 한다. 즉 도 2에서 예시한 반전 게이트 회로와 동일한 논리 회로이다.
- [0035] 도 3의 (b)에 나타난 바와 같이, 논리 신호에 의한 입력 전압의 변화에 따라 출력단 전압이 변화하고 있음에도, 전체 전류는 I_1 및 I_2 가 같다면, 일정하게 나타난다. 즉, 출력단(230)에 설치한 FET 소자가 논리 게이트와 동일한 특성을 갖는 소자이면 전체전류는 동일하게 되어 해밍 웨이트 값을 일정하게 유지시킨다. 즉, 해밍 웨이트 값에 의한 DPA 공격을 원천적으로 봉쇄하게 된다.
- [0036] 도 4는 본 발명에 따른 또 다른 실시예로서, 해밍 웨이트 모델을 이용한 전력 분석공격 방지 논리회로의 구성을 나타낸 회로도이다. 도 4에 나타난 바와 같이, 본 발명에 따른 전력 분석공격 방지 논리회로는 MOS형의 논리 게이트 회로와, 상기 논리 게이트 회로의 출력단에 설치되는 FET 소자와, 상기 논리 게이트 입력단에 설치되는 가변저항을 포함하되, 상기 가변저항의 조정을 통해 논리 회로 전체 전류를 일정하게 유지시키는 것을 특징으로 한다.
- [0037] 본 발명의 실시예는 도 4에 나타난 바와 같이, MOS형의 게이트(113) 회로 출력단에 FET 소자(210)를 설치하고, FET 소자의 소스와 V_{cc} 단자 연결 부위에 가변저항(215)을 연결하게 되면, 입력단 전압 V_{in} 에서 로직에 따라 0 또는 1을 번갈아 입력하게 되면, 전체 전류는 I_1 또는 I_2 로 나타나게 되는데, 상기 가변저항(215)을 조정하게 되면 I_1 과 I_2 를 동일하게 설정할 수 있게 되어, 결과적으로 전체 전류(I)를 일정하게 유지시킬 수 있게 된다.
- [0038] 그러므로, 본 발명의 실시예는 출력단에 FET 소자(210)와 가변저항(215)을 통해 논리 신호에 따른 전체 전류를 일정하게 유지시킴으로써, 해밍 웨이트 값에 의한 DPA 공격을 원천적으로 봉쇄할 수 있게 된다.
- [0039] 그리고, 본 발명에 따른 또 다른 실시예로서, 상술한 해밍 웨이트 모델을 이용한 전력 분석공격 방지 논리회로를 포함하는 스마트 카드를 제공함으로써 간단한 구성으로 보안 기능을 강화시킬 수 있게 된다.
- [0040] 이상의 설명에서 본 발명은 특정의 실시 예와 관련하여 도시 및 설명하였지만, 특허청구범위에 의해 나타난 발명의 사상 및 영역으로부터 벗어나지 않는 한도 내에서 다양한 개조 및 변화가 가능 하다는 것을 당 업계에서 통상의 지식을 가진 자라면 누구나 쉽게 알 수 있을 것이다.

도면

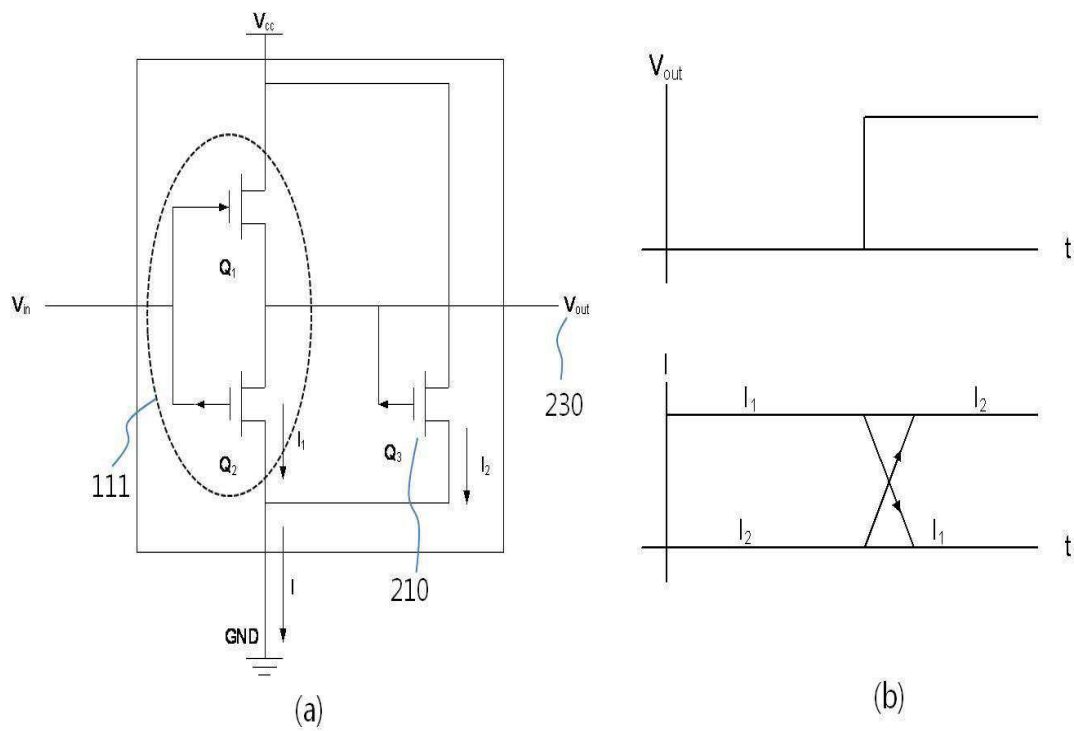
도면1



도면2



도면3



도면4

