(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.[6]
G08B 15/00

(11) 공개번호 특1997-0067025
(43) 공개일자 1997년10월13일

(21) 출원번호 특1997-0011151
(22) 출원일자 1997년03월28일
(30) 우선권주장 623,271 1996년03월28일 미국(US)
(71) 출원인 루센트 테크놀로지스 인코포레이티드 엘리 와이스
미합중국, 뉴저지 07974-0634, 머레이 힐, 마운틴 애비뉴 600
(72) 발명자 라그하바차리 퍼사
미합중국, 일리노이즈 60640, 시카고, 노쓰 매그놀리아 애비뉴 4637
(74) 대리인 이병호, 최달용

심사청구 : 없음

(54) VLSI 및 ULSI 장치의 도난 방지 방법 및 장치

요약

마이크로프로세서 및 DRAM 장치와 같은 VLSI 및 ULSI는 공장 및 창고로부터 대규모로 도난되기 쉽다. 도난을 감소시키는 제안된 방법은 이들 장치 내에 소량의 비휘방성 플래쉬 메모리를 포함한다. 플래쉬 메모리는 패스워드, 장치 일련번호 및 유저 식별 정보를 포함한다. 전원투입시, 장치는 표준 인터페이스를 통해, 패스워드화된 패스워드 검증 세션을 개시한다. 유저가 공급한 패스워드가 틀리면, 장치의 동작 포트(임의의 데이터 혹은 제어 출력 버스)는 3상태로 됨으로써, 장치를 사용할 수 없게 한다. 장치 일련번호 및 유저 식별 정보는 도난당한 장치를 찾았을 때 이 장치의 소유자를 판정함에서 있어 유용한 것이다.

대표도

도1

명세서

[발명의 명칭]

VLSI 및 ULSI 장치의 도난 방지 방법 및 장치

[도면의 간단한 설명]

제1도는 본 발명의 보안 기구의 일실시예를 갖는 장치의 블록도, 제2도는 제1도에 도시한 실시예의 비휘발성 플래쉬 메모리 구성을 도시한 도면, 제3도는 제1도에 도시한 실시예의 보안에 관련된 레지스터에 대한 블록도.

본 건은 요부공개 건이므로 전문 내용을 수록하지 않았음

(57) 청구의 범위

청구항 1

핵심 기능 회로 및 적어도 하나의 출력 포트를 갖는 대규모 집적 장치에 있어서, 상기 장치는 이에 대한 권한없는 사용을 방지하도록 상기 장치의 상기 핵심 기능을 제어하기 위한 내장형 보안 기구를 포함하는 것을 특징으로 하는 대규모 집적 장치.

청구항 2

제1항에 있어서, 상기 내장형 보안 기구는 상기 보안 기구의 동작을 제어하는 제어기; 상기 제어기에 전기적으로 결합되고, 상기 보안 기구와 외부 매개자간 인터페이스를 제공하는 경계 검사 포트; 상기 제어기에 전기적으로 결합되고, 소정의 저옵 및 데이터에 대한 비휘발성 저장소를 상기 보안 기구에 제공하는 플래쉬 메모리; 상기 제어기에 기능 지원을 제공하며, 상기 플래쉬 메모리, 상기 제어기 및 상기 경계 섬사 포트에 전기적으로 결합된 보안 레지스터 세트; 및 상기 핵심 기능 회로 및 상기 대규모 집적장치의 출력 포트들에 대한 기능 제어를 상기 제어기에 제공하며, 상기 제어기, 상기 핵심 기능 회로 및 상기 장치의 출력 포트들에 전기적으로 결합된 3상태 제어 로직을 포함하는 것을 특징으로 하는 대규모

집적 장치.

청구항 3

제2항에 있어서, 상기 제어기는 상기 외부 매개자가 보낸 명령들을 해석하며, 상기 플래쉬 메모리 및 상기 보안 레지스터를 유지관리하며, 상기 장치를 풀기위한 패스워드를 검증하고, 상기 외부 매개자에게 상기 소정의 데이터를 공급하며, 상기 3상태 로직을 통해 상기 핵심 기능 회로의 출력 포트를 제어하는 조합 로직 및 상태 머신 플립플롭을 포함하는 것을 특징으로 하는 대규모 집적 장치.

청구항 4

제2항에 있어서, 상기 플래쉬 메모리는 상기 소정의 정보 및 데이터를 저장하는 128바이트의 메모리를 제공하며, 상기 각각의 바이트는 8비트의 크기이며, 격리된 위치의 어드레스를 가지며, 상기 제1바이트는 위치 어드레스 0이며 마지막 바이트는 위치 어드레스 127인 것을 특징으로 하는 대규모 집적 장치.

청구항 5

제4항에 있어서, 상기 소정의 정보 및 데이터는 유저 식별 정보, 패스워드, 장치 일련번호, 랜덤 보안시도(challenge), 보안 세션 상태 정보 및 실패 정보를 포함하는 것을 특징으로 하는 대규모 집적 장치.

청구항 6

제5항에 있어서, 상기 보안 상태 정보는 위치 어드레스 0에 저장되며, 상기 실패 정보는 위치 어드레스 1 및 2에 저장되며, 상기 유저 식별 정보는 위치 어드레스 3-47에 저장되며, 상기 패스워드는 위치 어드레스 48-63에 저장되며, 상기 일련번호는 위치 어드레스 64-95에 저장되며, 상기 램점 보안 시도는 위치 어드레스 96-127에 저장되는 것을 특징으로 하는 대규모 집적 장치.

청구항 7

제5항에 있어서, 상기 랜덤 보안 시도는 테스트이며, 상기 테스트는 장치를 풀기 위해서 장치에 전원을 투입할 때마다 값을 복귀시키도록 상기 외부 매개자를 필요로 하는 것을 특징으로 하는 대규모 집적 장치.

청구항 8

제2항에 있어서, 상기 보안 레지스터는 보안 상태 레지스터, 보안 명령 레지스터, 페일러 임계치 레지스터, 페일러 카운트값 레지스터, 장치 패스워드 페지스터, 랜덤 시도 레지스터, 및 임시 데이터 레지스터를 포함하는 것을 특징으로 하는 대규모 집적 장치.

청구항 9

제2항에 있어서, 상기 경계 검사 포트는 표준 IEEE 1149.1 포트인 것을 특징으로 하는 대규모 집적 장치.

청구항 10

핵심 기능 회로 및 출력 포트들을 갖는 대규모 집적 장치의 내장형 보안기구에 있어서, 상기 보안 기구의 동작을 제어하는 제어기; 상기 제어기에 전기적으로 결합되고, 상기 보안 기구와 외부 매개자간 인터페이스를 제공하는 경계 검사 포트; 상기 제어기에 전기적으로 결합되고, 소정의 정보 및 데이터에 대한 비휘발성 저장소를 상기 보안 기구에 제공하는 플래쉬 메모리; 상기 제어기에 기능 지원을 제공하며, 상기 플래쉬 메모리, 상기 제어기 및 상기 경계 검사 포트에 전기적으로 결합된 보안 레지스터 세트; 및 상기 핵심 기능 회로 및 상기 대규모 집적장치의 출력포트들에 대한 기능 제어를 상기 제어기에 제공하며, 상기 제어기, 상기 핵심 기능 회로 및 상기 장치의 출력 포트들에 전기적으로 결합된 3상태 제어 로직을 포함하는 것을 특징으로 하는 대규모 집적 장치의 내장형 보안 기구.

청구항 11

제10항에 있어서, 상기 제어기는 상기 외부 매개자가 보낸 명령들을 해석하며, 상기 플래쉬 메모리 및 상기 보안 레지스터를 유지관리하며, 상기 장치를 풀기위한 패스워드를 검증하고, 상기 외부 매개자에게 상기 소정의 데이터를 공급하며, 상기 3상태 로직을 통해 상기 핵심 기능 회로의 출력 포트를 제어하는 조합로직 및 상태 머신 플립플롭을 포함하는 것을 특징으로하는 대규모 집적 장치의 내장형 보안 기구.

청구항 12

제11항에 있어서, 상기 플래스 메모리는 상기 소정의 정보 및 데이터를 저장하는 128바이트의 메모리를 제공하며, 상기 각각의 바이트는 8비트의 크기이며, 격리된 위치의 어드레스를 가지며, 상기 제1바이트는 위치 어드레스 0이며 마지막 바이트는 위치 어드레스 127인 것을 특징으로 하는 대규모 집적 장치의 내장형 보안 기구.

청구항 13

제12항에 있어서, 상기 소정의 정보 및 데이터는 유저 식별 정보, 패스워드, 장치 일련번호, 랜덤 보안시도, 보안 세션 상태 정보 및 실패 정보를 포함하는 것을 특징으로 하는 대규모 집적 장치의 내장형 보안 기구.

청구항 14

제13항에 있어서, 상기 보안 상태 정보는 위치 어드레스 0에 저장되며, 상기 실패 정보는 위치 어드레스

1 및 2에 저장되며, 상기 유저 식별 정보는 위치 어드레스 3-47에 저장되며, 상기 패스워드 위치 어드레스 48-63에 저장되며, 상기 일련번호는 위치 어드레스 64-95에 저장되며, 상기 랜점 보안 시도는 위치 어드레스 96-127에 저장되는 것을 특징으로 하는 대규모 집적 장치의 내장형 보안 기구.

청구항 15

제13항에 있어서, 상기 랜덤 보안 시도는 테스트이며, 상기 테스트는 장치를 풀기 위해서 장치에 전원을 투입할 때마다 값을 복귀시키도록 상기 외부 매개자를 필요로 하는 것을 특징으로 하는 대규모 집적 장치의 내장형 보안 기구.

청구항 16

제10항에 있어서, 상기 보안 레지스터는 보안 상태 레지스터, 보안 명령 레지스터, 패일러 임계치 레지스터, 페일러 카운트값 레지스터, 장치 패스워드 레지스터, 랜덤 시도 레지스터, 및 임시 데이터 레지스터를 포함하는것을 특징으로 하는 대규모 집적 장치의 내장형 보안 기구.

청구항 17

제16항에 있어서, 상기 경계 검사 포트는 표준 IEEE 1149.1포트인 것을 특징으로 하는 대규모 집적 장치의 내장형 보안 기구.

청구항 18

핵심 기능 회로 및 출력 포트들을 갖는 대규모 집적 장치의 도난으로부터 보호하는 방법에 있어서, 상기 방법은 상기 장치의 권한없는 사용으로부터 보호하기 위해 상기 장치에 보안 기구를 세우는 단계를 포함하는 것을 특징으로 하는 대규모 집적 장치의 도난 방지 방법.

청구항 19

제18항에 있어서, 상기 보안 기구는 외부 매개자로부터 상기 장치로의 권한없는 액세스에 대해 보호하도록 보안 세션에 진입하는 것을 특징으로 하는 대규모 집적 장치의 도난 방지 방법.

청구항 20

제19항에 있어서, 상기 보안 세션은 a. 상기 장치의 전원투입마다 패스워드를 복귀하도록 상기 매개자에게 요청하는 단계; b. 상기 보안 기구 내에 프로그램된 패스워드와 상기 복귀된 패스워드간 패스워드 일치가 존재하는지 여부를 결정하기 위해 상기 프로그램된 패스워드와 상기 복귀된 패스워드를 서로 비교하는 단계; c. 상기 패스워드 일치가 존재할 경우 상기 장치에 대한 상기 외부 매개자 액세스를 제공하는 단계를 포함하는 것을 특징으로 하는 대규모 집적 장치의 도난 방지 방법.

청구항 21

제19항에 있어서, 상기 보안 세션은 a. 상기 장치의 전원투입마다 랜덤 시도값을 복귀하도록 상기 매개자에게 요청하는 단계; b. 상기 보안 기구에 의해서 계산된 랜덤 시도값과 상기 복귀된 랜덤 시도값간의 시도값 일치가 존재하는지 여부를 결정하기 위해 상기 시도값과 상기 복귀된 랜덤 시도값을 서로 비교하는 단계; c. 상기 패스워드 일치가 존재할 경우 상기 장치에 대한 상기 외부 매개자 액세스를 제공하는 단계를 포함하는 것을 특징으로 하는 대규모 집적 장치의 도난 방지 방법.

청구항 22

제21항에 있어서, 상기 랜덤 시도값은 한 세트의 랜덤 변수로부터 상기외부 매개자와 상기 보안 기구에 의해서 계산된 값인 것을 특징으로 하는 대규모 집적 장치의 도난 방지 방법.

청구항 23

제19항에 있어서, 상기 보안 세션은 a. 상기 장치의 전원투입마다 패스워드 및 랜덤 시도값을 복귀하도록 상기 매개자에게 요청하는 단계; b. 상기 보안 기구에 의해서 계산된 랜덤 시도값과 상기 복귀된 랜덤 시도값간 시도값 일치가 존재하는지 여부를 결정하기 위해 상기 시도값과 상기 복귀된 랜덤 시도값을 서로 비교하는 단계; c. 상기 보안 기구 내에 프로그램된 패스워드와 상기 복귀된 패스워드간 패스워드 일치가 존재하는지 여부를 결정하기 위해 상기 프로그램된 패스워드와 상기 복귀된 패스워드는 서로 비교하는 단계; d.상기 시도값 일치 및 상기 패스워드 일치가 존재할 경우 상기 장치에 대한 상기 외부 매개자 액세스를 제공하는 단계를 포함하는 것을 특징으로 하는 대규모 집적 장치의 도난 방지 방법.

청구항 24

제19항에 있어서, 상기 보안 기구는 상기 외부 매개자가 상기 보안 세션을 통과한 경우 장치 일련번호 변경 세션에 진입하는 것을 특징으로 하는 대규모 집적 장치의 도난 방지 방법.

청구항 25

제19항에 있어서, 상기 보안 기구는 상기 외부 매개자가 상기 보안 세션을 통과한 경우 패스워드 변경세션에 진입하는 것을 특징으로 하는 대규모 집적 장치의 도난 방지 방법.

청구항 26

제19항에 있어서, 상기 보안 기구는 상기 외부 매개자가 상기 보안 세션을 통과한 경우 장치 일련번호 독출 세션에 진입하는 것을 특징으로 하는 대규모 집적 장치의 도난 방지 방법.

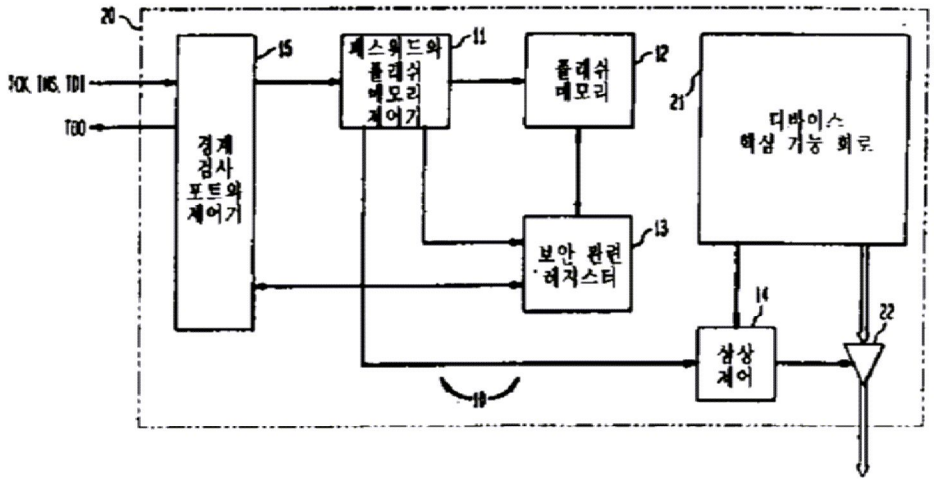
청구항 27

제19항에 있어서, 상기 보안 기구는 상기 외부 매개자가 상기 보안 세션을 통과한 경우 페일러 임계치 변경 세션에 진입하는 것을 특징으로 하는 대규모 집적 장치의 도난 방지 방법.

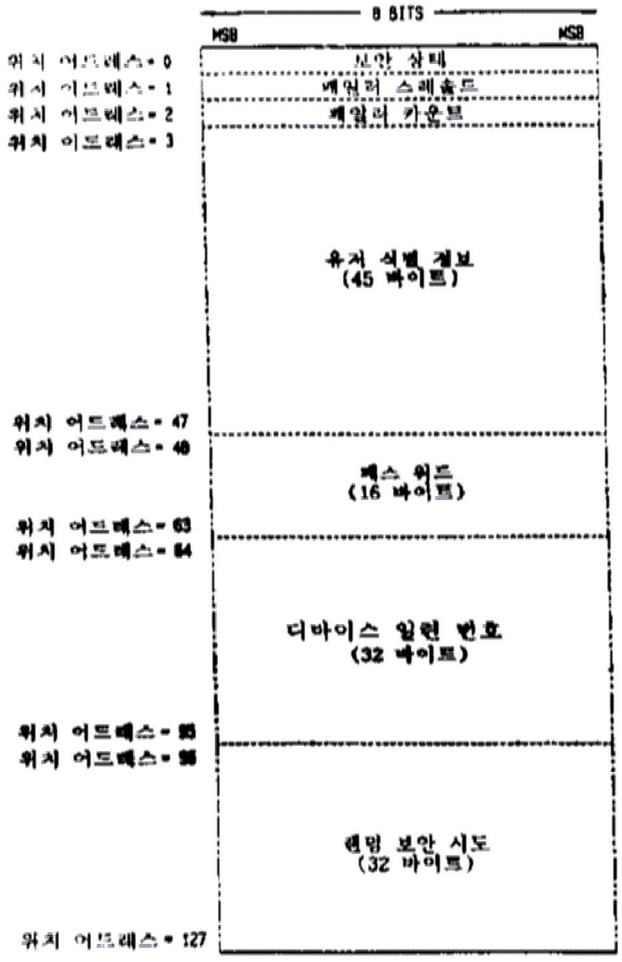
※ 참고사항 : 최초출원 내용에 의하여 공개하는 것임.

도면

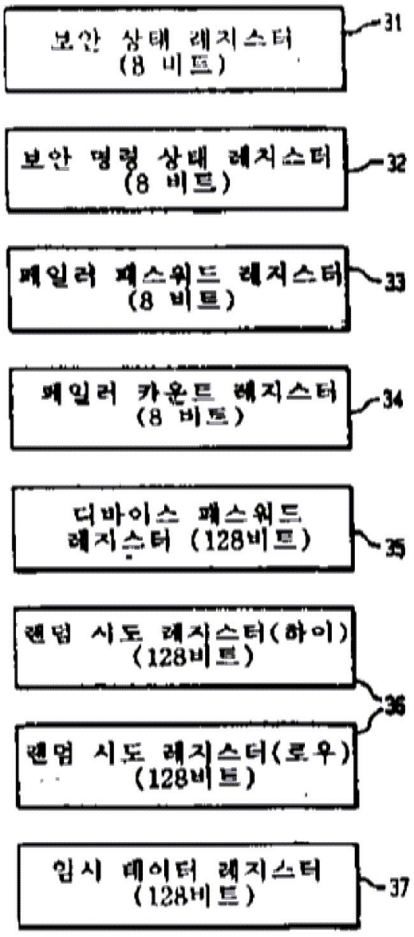
도면1



도면2



도면3


보안 상태 레지스터 (8 비트)
31
보안 명령 상태 레지스터 (8 비트)
32
페일러 패스워드 레지스터 (8 비트)
33
페일러 카운트 레지스터 (8 비트)
34
디바이스 패스워드 레지스터 (128비트)
35
랜덤 시도 레지스터(하이) (128비트)
36
랜덤 시도 레지스터(로우) (128비트)
임시 데이터 레지스터 (128비트)
37