(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.
G06F 12/14 (2006.01)
G06F 15/78 (2006.01)

(45) 공고일자 2007년01월09일
(11) 등록번호 10-0666328
(24) 등록일자 2007년01월03일

(21) 출원번호 10-2005-0011544
(22) 출원일자 2005년02월11일
심사청구일자 2005년02월15일

(65) 공개번호 10-2006-0090859
(43) 공개일자 2006년08월17일

(73) 특허권자 삼성전자주식회사
경기도 수원시 영통구 매탄동 416

(72) 발명자 서윤범
서울 동작구 사당5동 231-12

공명석
경기 수원시 영통구 매탄3동 1250-5 206호

민병호
서울 강남구 압구정동 신현대아파트 126동 703호

(74) 대리인 박영우

(56) 선행기술조사문헌
JP2000163547 A
JP2003209545 A
KR1020010098800 A *
US20050033951 A1
JP2001256114 A
KR1020000052797 A
KR1020020085753 A
* 심사관에 의하여 인용된 문헌

심사관 : 이종익

전체 청구항 수 : 총 41 항

(54) 온 칩 메모리를 이용한 기밀 정보 보안 장치 및 보안 방법

(57) 요약

제 1 보안키를 소정 영역에 저장하는 온 칩 메모리부, 제 2 보안키를 저장하는 제 2 보안키 저장부, 칩 내부로부터 온 칩 메모리부에 대한 억세스 신호를 발생시키는 메모리 컨트롤러, 칩 외부로부터 온 칩 메모리부에 대한 억세스를 요청하기 위한 테스트 인에이블 신호와 온 칩 메모리부에 대한 억세스 신호를 수신하는 외부 입출력 핀, 온 칩 메모리부로부터 메모리 컨트롤러를 통하여 제 1 보안키를 읽어들이고, 제 2 보안키 저장부로부터 제 2 보안키를 읽어들여 비교하고 보안키 비교 신호를 출력하는 비교 로직부, 및 보안키 비교 신호에 응답하여, 외부 입출력 핀을 통하여 수신된 온 칩 메모리부에 대한 억세스 신호의 허용 여부를 결정하는 억세스 제어부를 포함하여 온 칩 메모리를 이용한 기밀 정보 보안 장치를 구성한다. 따라서, 제품의 생산 과정에서는 기밀 정보의 저장 및 변경을 가능하게 하고, 제품이 출하된 다음에는 기밀 정보의 파괴 및 유출을 방지할 수 있도록 하는 효과가 있다.

대표도

도 2

특허청구의 범위

청구항 1.

제 1 보안키를 소정 영역에 저장하는 온 칩 메모리부;

제 2 보안키를 저장하는 제 2 보안키 저장부;

칩 내부로부터 상기 온 칩 메모리부에 대한 억세스 신호를 발생시키는 메모리 컨트롤러;

칩 외부로부터 상기 온 칩 메모리부에 대한 억세스를 요청하기 위한 테스트 인에이블 신호와 상기 온 칩 메모리부에 대한 억세스 신호를 수신하는 외부 입출력 핀;

상기 온 칩 메모리부로부터 상기 메모리 컨트롤러를 통하여 상기 제 1 보안키를 읽어들이고, 상기 제 2 보안키 저장부로부터 상기 제 2 보안키를 읽어들여 비교하고 보안키 비교 신호를 출력하는 비교 로직부; 및

상기 보안키 비교 신호에 응답하여, 상기 외부 입출력 핀을 통하여 수신된 상기 온 칩 메모리부에 대한 억세스 신호의 허용 여부를 결정하는 억세스 제어부를 포함한 것을 특징으로 하는 온 칩 메모리를 이용한 기밀 정보 보안 장치.

청구항 2.

제 1 항에 있어서,

상기 외부 입출력 핀은

상기 테스트 인에이블 신호를 수신하는 테스트 인에이블 신호 입력핀; 및

상기 온 칩 메모리부에 대한 억세스 신호를 입출력 하기 위한 억세스 신호 입출력 핀을 포함한 것을 특징으로 하는 온 칩 메모리를 이용한 기밀 정보 보안 장치.

청구항 3.

제 2 항에 있어서,

상기 온 칩 메모리부에 대한 억세스 신호는

상기 온 칩 메모리부에 대한 어드레스 신호;

상기 온 칩 메모리부에 대한 제어 신호; 및

상기 온 칩 메모리부에 대한 데이터 신호를 포함하여 구성된 것을 특징으로 하는 온 칩 메모리를 이용한 기밀 정보 보안 장치.

청구항 4.

제 1 항에 있어서,

상기 비교 로직부는

상기 메모리 컨트롤러를 통하여, 상기 온 칩 메모리부의 상기 소정 영역에 기록된 제 1 보안키를 읽어들여 저장하고 출력하는 레지스터부; 및

상기 레지스터부로부터 출력된 제 1 보안키를 상기 제 2 보안키 저장부에서 읽어들인 제 2 보안키와 비교하여 상기 보안키 비교 신호를 출력하는 비교부를 포함하여 구성된 것을 특징으로 하는 온 칩 메모리를 이용한 기밀 정보 보안 장치.

청구항 5.

제 1 항에 있어서,

상기 비교 로직부는

상기 메모리 컨트롤러를 통하여, 상기 온 칩 메모리부의 상기 소정 영역에 기록된 제 1 보안키를 읽어들여 출력하는 비교 제어부; 및

상기 비교 제어부로부터 출력된 제 1 보안키를 상기 제 2 보안키 저장부에서 읽어들인 제 2 보안키와 비교하여 상기 보안키 비교 신호를 출력하는 비교부를 포함하여 구성된 것을 특징으로 하는 온 칩 메모리를 이용한 기밀 정보 보안 장치.

청구항 6.

제 1 항에 있어서,

상기 비교 로직부는

상기 제 1 보안키와 상기 제 2 보안키가 동일한 경우에는 '로우'인 보안키 비교 신호를 출력하고, 상기 제 1 보안키와 상기 제 2 보안키가 상이한 경우에는 '하이'인 보안키 비교 신호를 출력하도록 구성된 특징으로 하는 온 칩 메모리를 이용한 기밀 정보 보안 장치.

청구항 7.

제 1 항에 있어서,

상기 억세스 제어부는

상기 비교 로직부로부터 상기 보안키 비교 신호를 수신하고, 상기 외부 입출력 핀으로부터 상기 테스트 인에이블 신호를 수신하여 논리 연산한 억세스 선택 신호를 출력하는 논리 연산부; 및

상기 억세스 선택 신호에 응답하여, 상기 외부 입출력 핀을 통하여 수신한 상기 온 칩 메모리부에 대한 억세스 신호의 상기 온 칩 메모리부로의 전달 여부를 결정하는 인터페이스부를 포함한 것을 특징으로 하는 온 칩 메모리를 이용한 기밀 정보 보안 장치.

청구항 8.

제 7 항에 있어서,

상기 논리 연산부는

상기 보안키 비교 신호가 상기 제 1 보안키와 상기 제 2 보안키가 상이함을 지시하고, 상기 테스트 인에이블 신호가 활성화되었을 때, 활성화된 억세스 선택 신호를 출력하는 논리 연산 소자를 포함하여 구성된 것을 특징으로 하는 온 칩 메모리를 이용한 기밀 정보 보안 장치.

청구항 9.

제 7 항에 있어서,

상기 인터페이스부는

상기 억세스 선택 신호에 응답하여, 상기 메모리 컨트롤러에서 발생된 상기 온 칩 메모리부에 대한 억세스 신호와 상기 외부 입출력 핀을 통하여 수신한 상기 온 칩 메모리부에 대한 억세스 신호를 선택적으로 상기 온 칩 메모리부에 전달하는 다중화 로직을 포함하여 구성된 것을 특징으로 하는 온 칩 메모리를 이용한 기밀 정보 보안 장치.

청구항 10.

제 1 항에 있어서,

상기 메모리 컨트롤러는,

상기 제 1 보안키를 상기 온 칩 메모리부의 상기 소정 영역에서 읽어들여 상기 비교 로직부에 전달하는 중에는 비활성화되고, 모두 전달했을 경우에는 활성화되는 로드 완료 신호를 상기 억세스 제어부로 출력하는 것을 특징으로 하는 온 칩 메모리를 이용한 기밀 정보 보안 장치.

청구항 11.

제 10 항에 있어서,

상기 억세스 제어부는

상기 비교 로직부로부터 상기 보안키 비교 신호를 수신하고, 상기 외부 입출력 핀으로부터 상기 테스트 인에이블 신호를 수신하고, 상기 메모리 컨트롤러로부터 상기 로드 완료 신호를 수신하여 논리 연산한 억세스 선택 신호를 출력하는 논리 연산부; 및

상기 억세스 선택 신호에 응답하여, 상기 외부 입출력 핀을 통하여 수신한 상기 온 칩 메모리부에 대한 억세스 신호의 상기 온 칩 메모리부로의 전달 여부를 결정하는 인터페이스부를 포함한 것을 특징으로 하는 온 칩 메모리를 이용한 기밀 정보 보안 장치.

청구항 12.

제 11 항에 있어서,

상기 논리 연산부는

상기 보안키 비교 신호가 상기 제 1 보안키와 상기 제 2 보안키가 상이함을 지시하고, 상기 테스트 인에이블 신호가 활성화되었으며, 상기 로드 완료 신호가 활성화되었을 때, 활성화된 억세스 선택 신호를 출력하는 논리 연산 소자를 포함하여 구성된 것을 특징으로 하는 온 칩 메모리를 이용한 기밀 정보 보안 장치.

청구항 13.

제 11 항에 있어서,

상기 인터페이스부는

상기 억세스 선택 신호에 응답하여, 상기 메모리 컨트롤러에서 발생된 상기 온 칩 메모리부에 대한 억세스 신호와 상기 외부 입출력 핀을 통하여 수신한 상기 온 칩 메모리부에 대한 억세스 신호를 선택적으로 상기 온 칩 메모리부에 전달하는 다중화 로직을 포함하여 구성된 것을 특징으로 하는 온 칩 메모리를 이용한 기밀 정보 보안 장치.

청구항 14.

제 1 항에 있어서,

상기 온 칩 메모리부는

비휘발성 멀티-타임 프로그래머블 메모리 셀 어레이로 구성된 것을 특징으로 하는 온 칩 메모리를 이용한 기밀 정보 보안 장치.

청구항 15.

제 14 항에 있어서,

상기 온 칩 메모리부는

플래쉬 메모리 셀 어레이로 구성된 것을 특징으로 하는 온 칩 메모리를 이용한 기밀 정보 보안 장치.

청구항 16.

제 1 항에 있어서,

상기 제 2 보안키 저장부는

하드 와이어드 방식에 의해서 구현된 것을 특징으로 하는 온 칩 메모리를 이용한 기밀 정보 보안 장치.

청구항 17.

제 1 항에 있어서,

상기 제 2 보안키 저장부는

마스크 롬을 이용하여 구현된 것을 특징으로 하는 하드 와이어드 방식에 의해서 구현된 것을 특징으로 하는 온 칩 메모리를 이용한 기밀 정보 보안 장치.

청구항 18.

제 1 보안키와 제 2 보안키를 소정 영역에 저장하는 온 칩 메모리부;

칩 내부로부터 상기 온 칩 메모리부에 대한 억세스 신호를 발생시키는 메모리 컨트롤러;

칩 외부로부터 상기 온 칩 메모리부에 대한 억세스를 요청하기 위한 테스트 인에이블 신호와 상기 온 칩 메모리부에 대한 억세스 신호를 수신하는 외부 입출력 핀;

상기 온 칩 메모리부로부터 상기 메모리 컨트롤러를 통하여 상기 제 1 보안키와 상기 제 2 보안키를 읽어들여 비교하고 보안키 비교 신호를 출력하는 비교 로직부; 및

상기 보안키 비교 신호에 응답하여, 상기 외부 입출력 핀을 통하여 수신된 상기 온 칩 메모리부에 대한 억세스 신호의 허용 여부를 결정하는 억세스 제어부를 포함한 것을 특징으로 하는 온 칩 메모리를 이용한 기밀 정보 보안 장치.

청구항 19.

제 18 항에 있어서,

상기 외부 입출력 핀은

상기 테스트 인에이블 신호를 수신하는 테스트 인에이블 신호 입력핀; 및

상기 온 칩 메모리부에 대한 억세스 신호를 입출력 하기 위한 억세스 신호 입출력 핀을 포함한 것을 특징으로 하는 온 칩 메모리를 이용한 기밀 정보 보안 장치.

청구항 20.

제 19 항에 있어서,

상기 온 칩 메모리부에 대한 억세스 신호는

상기 온 칩 메모리부에 대한 어드레스 신호;

상기 온 칩 메모리부에 대한 제어 신호; 및

상기 온 칩 메모리부에 대한 데이터 신호를 포함하여 구성된 것을 특징으로 하는 온 칩 메모리를 이용한 기밀 정보 보안 장치.

청구항 21.

제 18 항에 있어서,

상기 비교 로직부는

상기 메모리 컨트롤러를 통하여, 상기 온 칩 메모리부의 상기 소정 영역에 기록된 제 1 보안키를 읽어들여 저장하고 출력하는 제 1 레지스터부;

상기 메모리 컨트롤러를 통하여, 상기 온 칩 메모리부의 상기 소정 영역에 기록된 제 2 보안키를 읽어들여 저장하고 출력하는 제 2 레지스터부; 및

상기 제 1 레지스터부로부터 출력된 제 1 보안키를 상기 제 2 레지스터부로부터 출력된 제 2 보안키와 비교하여 상기 보안키 비교 신호를 출력하는 비교부를 포함하여 구성된 것을 특징으로 하는 온 칩 메모리를 이용한 기밀 정보 보안 장치.

청구항 22.

제 21 항에 있어서,

상기 제 1 레지스터부와 상기 제 2 레지스터부 중의 적어도 하나는

적어도 하나의 비트에 연결된 퓨즈를 포함하고, 상기 퓨즈는 상기 퓨즈가 연결된 비트의 상태를 '0' 또는 '1'로 고정시키는 역할을 수행하는 것을 특징으로 하는 온 칩 메모리를 이용한 기밀 정보 보안 장치.

청구항 23.

제 22 항에 있어서,

상기 퓨즈는 전기적 퓨즈인 것을 특징으로 하는 온 칩 메모리를 이용한 기밀 정보 보안 장치.

청구항 24.

제 18 항에 있어서,

상기 비교 로직부는

상기 제 1 보안키와 상기 제 2 보안키가 동일한 경우에는 '로우'인 보안키 비교 신호를 출력하고, 상기 제 1 보안키와 상기 제 2 보안키가 상이한 경우에는 '하이'인 보안키 비교 신호를 출력하도록 구성된 특징으로 하는 온 칩 메모리를 이용한 기밀 정보 보안 장치.

청구항 25.

제 18 항에 있어서,

상기 억세스 제어부는

상기 비교 로직부로부터 상기 보안키 비교 신호를 수신하고, 상기 외부 입출력 핀으로부터 상기 테스트 인에이블 신호를 수신하여 논리 연산한 억세스 선택 신호를 출력하는 논리 연산부; 및

상기 억세스 선택 신호에 응답하여, 상기 외부 입출력 핀을 통하여 수신한 상기 온 칩 메모리부에 대한 억세스 신호의 상기 온 칩 메모리부로의 전달 여부를 결정하는 인터페이스부를 포함한 것을 특징으로 하는 온 칩 메모리를 이용한 기밀 정보 보안 장치.

청구항 26.

제 25 항에 있어서,

상기 논리 연산부는

상기 보안키 비교 신호가 상기 제 1 보안키와 상기 제 2 보안키가 상이함을 지시하고, 상기 테스트 인에이블 신호가 활성화되었을 때, 활성화된 억세스 선택 신호를 출력하는 논리 연산 소자를 포함하여 구성된 것을 특징으로 하는 온 칩 메모리를 이용한 기밀 정보 보안 장치.

청구항 27.

제 25 항에 있어서,

상기 인터페이스부는

상기 억세스 선택 신호에 응답하여, 상기 메모리 컨트롤러에서 발생된 상기 온 칩 메모리부에 대한 억세스 신호와 상기 외부 입출력 핀을 통하여 수신한 상기 온 칩 메모리부에 대한 억세스 신호를 선택적으로 상기 온 칩 메모리부에 전달하는 다중화 로직을 포함하여 구성된 것을 특징으로 하는 온 칩 메모리를 이용한 기밀 정보 보안 장치.

청구항 28.

제 18 항에 있어서,

상기 메모리 컨트롤러는,

상기 제 1 보안키와 상기 제 2 보안키를 상기 온 칩 메모리부의 상기 소정 영역에서 읽어들여 상기 비교 로직부에 전달하는 중에는 비활성화되고, 모두 전달했을 경우에는 활성화되는 로드 완료 신호를 상기 억세스 제어부로 출력하는 것을 특징으로 하는 온 칩 메모리를 이용한 기밀 정보 보안 장치.

청구항 29.

제 28 항에 있어서,

상기 억세스 제어부는

상기 비교 로직부로부터 상기 보안키 비교 신호를 수신하고, 상기 외부 입출력 핀으로부터 상기 테스트 인에이블 신호를 수신하고, 상기 메모리 컨트롤러로부터 상기 로드 완료 신호를 수신하여 논리 연산한 억세스 선택 신호를 출력하는 논리 연산부; 및

상기 억세스 선택 신호에 응답하여, 상기 외부 입출력 핀을 통하여 수신한 상기 온 칩 메모리부에 대한 억세스 신호의 상기 온 칩 메모리부로의 전달 여부를 결정하는 인터페이스부를 포함한 것을 특징으로 하는 온 칩 메모리를 이용한 기밀 정보 보안 장치.

청구항 30.

제 29 항에 있어서,

상기 논리 연산부는

상기 보안키 비교 신호가 상기 제 1 보안키와 상기 제 2 보안키가 상이함을 지시하고, 상기 테스트 인에이블 신호가 활성화되었으며, 상기 로드 완료 신호가 활성화되었을 때, 활성화된 억세스 선택 신호를 출력하는 논리 연산 소자를 포함하여 구성된 것을 특징으로 하는 온 칩 메모리를 이용한 기밀 정보 보안 장치.

청구항 31.

제 29 항에 있어서,

상기 인터페이스부는

상기 억세스 선택 신호에 응답하여, 상기 메모리 컨트롤러에서 발생된 상기 온 칩 메모리부에 대한 억세스 신호와 상기 외부 입출력 핀을 통하여 수신한 상기 온 칩 메모리부에 대한 억세스 신호를 선택적으로 상기 온 칩 메모리부에 전달하는 다중화 로직을 포함하여 구성된 것을 특징으로 하는 온 칩 메모리를 이용한 기밀 정보 보안 장치.

청구항 32.

제 18 항에 있어서,

상기 온 칩 메모리부는

비휘발성 멀티-타임 프로그래머블 메모리 셀 어레이로 구성된 것을 특징으로 하는 온 칩 메모리를 이용한 기밀 정보 보안 장치.

청구항 33.

제 18 항에 있어서,

상기 온 칩 메모리부는

플래쉬 메모리 셀 어레이로 구성된 것을 특징으로 하는 온 칩 메모리를 이용한 기밀 정보 보안 장치.

청구항 34.

제 1 보안키와 제 2 보안키를 비교하는 보안키 비교 단계;

칩 외부로부터 온 칩 메모리부에 대한 억세스 요청을 수신하는 단계;

상기 제 1 보안키와 상기 제 2 보안키가 동일한 경우에는 상기 억세스 요청을 차단하는 단계; 및

상기 제 1 보안키와 상기 제 2 보안키가 상이한 경우에는 상기 억세스 요청에 응답하여 상기 온 칩 메모리부에 대한 억세스를 수행하고, 상기 제 1 보안키를 상기 제 2 보안키와 동일한 길이와 내용을 가진 비트열이 되도록 상기 온 칩 메모리부에 기록하는 단계를 포함한 온 칩 메모리 장치를 이용한 기밀 정보 보안 방법.

청구항 35.

제 34 항에 있어서,

상기 온 칩 메모리부에 대한 억세스를 수행하는 단계는 상기 제 1 보안키를 상기 온 칩 메모리부의 소정 영역에 읽거나 쓰는 동작을 수행할 수 있는 것을 특징으로 하는 온 칩 메모리 장치를 이용한 기밀 정보 보안 방법.

청구항 36.

제 34 항에 있어서,

상기 온 칩 메모리부에 대한 억세스를 수행하는 단계는 상기 제 2 보안키를 상기 온 칩 메모리부의 소정 영역에 읽거나 쓰는 동작을 수행할 수 있는 것을 특징으로 하는 온 칩 메모리 장치를 이용한 기밀 정보 보안 방법.

청구항 37.

제 34 항에 있어서,

상기 기밀 정보 보안 방법은

상기 보안키 비교 단계의 진행 중에는 상기 칩 외부로부터 온 칩 메모리부에 대한 억세스 요청을 차단하는 단계를 추가로 포함한 것을 특징으로 하는 온 칩 메모리 장치를 이용한 기밀 정보 보안 방법.

청구항 38.

제 34 항에 있어서,

상기 보안키 비교 단계에서는 상기 제 1 보안키와 상기 제 2 보안키가 동일한 경우에는 비활성화된 보안키 비교 신호를 출력하고, 상기 제 1 보안키와 상기 제 2 보안키가 상이한 경우에는 활성화된 보안키 비교 신호를 출력하는 것을 특징으로 하는 온 칩 메모리 장치를 이용한 기밀 정보 보안 방법.

청구항 39.

제 38 항에 있어서,

상기 억세스 요청을 차단하는 단계와 상기 억세스 요청에 응답하여 상기 온 칩 메모리부에 대한 억세스를 수행하는 단계는 상기 보안키 비교 신호에 응답하여 이루어지는 것을 특징으로 하는 온 칩 메모리 장치를 이용한 기밀 정보 보안 방법.

청구항 40.

제 38 항에 있어서,

상기 보안키 비교 단계는 상기 온 칩 메모리 장치를 이용한 기밀 정보 보안 방법이 수행되는 칩이 파워 온 되거나, 리셋될 때마다 이루어지는 것을 특징으로 하는 온 칩 메모리 장치를 이용한 기밀 정보 보안 방법.

청구항 41.

제 40 항에 있어서,

상기 보안키 비교 신호는 상기 칩이 다시 파워 다운되거나, 리셋될 때까지 상태가 유지되는 것을 특징으로 하는 온 칩 메모리 장치를 이용한 기밀 정보 보안 방법.

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 기밀 정보의 보안 장치 및 보안 방법에 대한 것으로, 더 자세하게는, 기밀 정보의 유출 및 파괴를 방지할 수 있도록 하는 온 칩 메모리 장치를 이용한 기밀 정보 보안 장치 및 보안 방법에 관한 것이다.

컴퓨터 기술 및 통신 기술의 발전에 따라서, 다양한 목적과 이유에 의해서 각각의 장치들은 고유의 기밀 정보를 저장하고, 이를 이용하여 장치들 상호간에 인증을 하거나, 장치들 각각이 개별적으로 인식되는 절차가 필요해지고 있다.

상기한 기밀 정보의 대표적인 예로는, 상업화된 프로토콜(protocol)에 대한 불법적인 사용을 방지하기 위해서 프로토콜 라이센스(protocol license)를 허여받은 장치에 대해서만 프로토콜의 사용을 허용하는 경우에, 프로토콜을 사용하는 장치들 간의 고유 인증 절차에 이용되는 인증키(authentification key)를 들 수 있다. 또는, 개별적으로 식별되어야하는 장치들을 식별(identification)하기 위해서 부여되는 장치의 고유 번호 등이 상기 기밀 정보에 포함될 수 있다.

한편, 이하에서 상기 기밀 정보를 대표하는 용어로서 '인증키'가 사용될 수 있으나, 좁은 의미의 인증키에 한정되지 않고 넓은 의미로 해석되어 인증키를 포함한 기밀 정보의 의미를 내포하는 것으로 사용되는 것임을 미리 밝힌다.

인증키를 포함한 기밀 정보들은 장치들마다 그 내용이 다른 것이 일반적이며, 제품이 시장에 출시되기 전, 예컨대 제품 생산 과정의 최종 단계에서 제품에 기록된다.

따라서, 이와 같은 인증키를 개별 장치들에 기록하기 위해서 다양한 방법이 종래에 존재하였다.

첫째는, 메인 칩 외부에 별도의 외부 메모리 장치를 구비하여 인증키를 저장하는 방식이다. 장치들마다 개별적으로 상이한 인증키가 부여되기 때문에 장치의 메인 칩 내부에 존재하는 온 칩 마스크 롬(on-chip mask ROM)등에 인증키를 기록하는 것은 문제가 된다. 장치들마다 상이한 인증키를 메인 칩 내에 존재하는 마스크 롬 상에 기록하는 것은 공정 상, 비용 상 어려움이 있기 때문이다. 여기에서, 별도의 외부 메모리 장치로는, 특히 비휘발성 특성(NV; Non-Volatile)을 가지는 플래쉬 메모리 장치가 널리 사용된다. 예컨대, 별도의 외부 메모리 장치를 사용하여 인증키를 암호화(encryption)하여 저장하고, 별도의 외부 메모리 장치에는 인증키를 기록한 부분에 대한 쓰기 보호(write protection) 등을 하는 방식이다. 즉, 별도 외부 메모리 장치의 특정 핀을 본딩(bonding)하는 방식 등으로 인증키에 대한 접근을 막는 방식이다.

그러나, 이러한 방식의 경우, 외부 메모리 장치에 인증키가 저장되므로, 장치로부터 외부 메모리 장치를 분리하여 외부 메모리 장치에 접근하는 방식을 이용하여 인증키를 해독하거나 파괴하는 경우에 대해서는 대처할 수 없다는 문제점이 있다.

둘째로, 외부 메모리 장치에 인증키를 저장하는 경우의 보안상 문제를 해결하기 위해서 메인 칩 내부에 포함된 (embedded) 온 칩 메모리 장치에 인증키를 저장하는 방식이 사용된다.

온 칩 메모리 장치로는 비휘발성 특성을 가지면서도 재프로그래밍(re-programming)이 가능한 플래쉬(flash) 메모리 장치들이 사용된다. 이때, 제품의 생산 과정에서는 온 칩 메모리 장치에 인증키를 기입하거나 변경이 가능하도록 하고, 인증키의 기입이 완료되면 더 이상 외부에서는 온 칩 메모리 장치에 기입된 인증키에 접근을 할 수 없도록 하여야 한다.

도1은 종래 기술의 온 칩 메모리 장치를 이용한 기밀 정보 보안 장치의 블록도이다.

도1을 참조하면, 종래 기술의 기밀 정보 보안 장치(100)는 온 칩 메모리부(101), 메모리 컨트롤러(102), 테스트 인터페이스부(103) 및 외부 입출력 핀들(104)을 포함하여 구성된다.

온 칩 메모리부(101)는 비휘발성이고 재프로그래밍이 가능한 플래쉬 메모리 셀 어레이가 포함되어 구현될 수 있음은 이미 언급된 바와 같다. 이때, 상기 메모리 컨트롤러(102)는 플래쉬 메모리 셀 어레이를 제어 가능한 플래쉬 메모리 컨트롤러가 된다.

한편, 제품의 생산 과정에서 온 칩 메모리부(101)에 인증키 등의 기밀 정보를 기입하거나 변경하는 것이 가능하도록 하기 위해서, 기밀 정보 보안 장치(100)는 외부 입출력 핀들(104)을 가진다. 여기에서, 외부 입출력 핀들(104)은 테스트 인에이블 신호(TEST_EN)를 입력받기 위한 핀(TEST_EN_PIN)과 온 칩 메모리부(101)를 억세스하기 위한 어드레스 신호(E_ADDR)를 입력받는 어드레스 신호 핀(E_ADDR_PIN), 제어 신호(E_CTRL)를 입력받는 제어 신호 핀(E_CTRL_PIN), 및 데이터 신호(E_DIO)를 입출력하는 데이터 신호 핀(E_DIO_PIN)들로 구성된다.

외부에서 온 칩 메모리부(101)에 기밀 정보를 기입하거나 변경하기 위해서는 테스트 인에이블 핀(TEST_EN_PIN)을 통하여 활성화된 테스트 인에이블 신호(TEST_EN)를 입력한다. 이때, 테스트 인터페이스부(103)는 테스트 인에이블 신호(TEST_EN)의 상태에 따라서 인에이블(enable) 여부가 결정된다.

테스트 인에이블 신호(TEST_EN)가 활성화된 경우에는 테스트 인터페이스부(103)가 인에이블(enable)되어 상기 외부 입출력 핀들(104)로부터 입력된 억세스 신호들(E_ADDR, E_CTRL, E_DIO)을 온 칩 메모리부(101)에 전달한다. 즉, 제품의 생산 과정에서는 테스트 인에이블 신호(TEST_EN)를 입력하여 기밀 정보를 기록하거나 변경할 수 있다.

반대로, 테스트 인에이블 신호(TEST_EN)가 비활성화된 경우에는 테스트 인터페이스부(103)가 디스인에이블(disenable)되어 상기 외부 입출력 핀들(104)로부터 입력된 억세스 신호들(E_ADDR, E_CTRL, E_DIO)이 온 칩 메모리부(101)에 전달되지 않고 차단된다. 따라서, 일단 기밀 정보가 기록되면 테스트 인에이블 핀(TEST_EN_PIN)을 비활성화 상태로 고정시킴으로써 칩 외부로부터 온 칩 메모리부(101)로의 접근을 차단하는 것이다.

그러나, 이러한 기밀 정보 보안 장치의 경우에도, 약간의 핀 조작을 통해 기밀 정보의 유출이나 파괴가 가능한 문제점이 존재한다. 예컨대, 제품 생산 과정에서 기밀 정보를 기록한 다음에 테스트 인에이블 핀(TEST_EN_PIN)을 고정한다고 하더라도, 칩 자체를 분리하여 테스트 인에이블 핀(TEST_EN_PIN)을 활성화상태로 바이어싱(biasing)하면, 재차 외부에서 온 칩 메모리부에 대한 억세스가 가능해진다. 따라서, 종래 기술과 같이 온 칩 메모리 장치를 이용하는 것만으로는 기밀 정보를 보호할 수 없으며, 온 칩 메모리 장치에 대해서 외부 핀을 이용하여 기밀 정보를 기록 또는 변경을 하도록 설계된 경우에는 기밀 정보에 대한 별도의 보안책이 강구되어야만 한다.

발명이 이루고자 하는 기술적 과제

상기와 같은 문제점을 해결하기 위해서 본 발명의 목적은, 생산 과정에서는 기밀 정보의 저장 및 변경을 가능하게 하고, 제품이 출하된 다음에는 기밀 정보의 파괴 및 유출을 방지할 수 있도록 하는 온 칩 메모리 장치를 이용한 기밀 정보 보안 장치를 제공하는데 있다.

본 발명의 또 다른 목적은, 생산 과정에서는 기밀 정보의 저장 및 변경을 가능하게 하고, 제품이 출하된 다음에는 기밀 정보의 파괴 및 유출을 방지할 수 있도록 하는 온 칩 메모리 장치를 이용한 기밀 정보 보안 방법을 제공하는데 있다.

발명의 구성

상기 목적을 달성하기 위해 본 발명의 한 형태는, 제 1 보안키를 소정 영역에 저장하는 온 칩 메모리부, 제 2 보안키를 저장하는 제 2 보안키 저장부, 칩 내부로부터 상기 온 칩 메모리부에 대한 억세스 신호를 발생시키는 메모리 컨트롤러, 칩 외부로부터 상기 온 칩 메모리부에 대한 억세스를 요청하기 위한 테스트 인에이블 신호와 상기 온 칩 메모리부에 대한 억세스 신호를 수신하는 외부 입출력 핀, 상기 온 칩 메모리부로부터 상기 메모리 컨트롤러를 통하여 상기 제 1 보안키를 읽어들이고, 상기 제 2 보안키 저장부로부터 상기 제 2 보안키를 읽어들여 비교하고 보안키 비교 신호를 출력하는 비교 로직부, 및 상기 보안키 비교 신호에 응답하여, 상기 외부 입출력 핀을 통하여 수신된 상기 온 칩 메모리부에 대한 억세스 신호의 허용 여부를 결정하는 억세스 제어부를 포함한 것을 특징으로 하는 온 칩 메모리를 이용한 기밀 정보 보안 장치를 제공한다.

여기에서, 상기 외부 입출력 핀은 상기 테스트 인에이블 신호를 수신하는 테스트 인에이블 신호 입력핀 및 상기 온 칩 메모리부에 대한 억세스 신호를 입출력 하기 위한 억세스 신호 입출력 핀을 포함하여 구성될 수 있다.

여기에서, 상기 비교 로직부는 상기 메모리 컨트롤러를 통하여, 상기 온 칩 메모리부의 상기 소정 영역에 기록된 제 1 보안키를 읽어들여 저장하고 출력하는 레지스터부, 및 상기 레지스터부로부터 출력된 제 1 보안키를 상기 제 2 보안키 저장부에서 읽어들인 제 2 보안키와 비교하여 상기 보안키 비교 신호를 출력하는 비교부를 포함하여 구성될 수 있다.

여기에서, 상기 비교 로직부는 상기 메모리 컨트롤러를 통하여, 상기 온 칩 메모리부의 상기 소정 영역에 기록된 제 1 보안키를 읽어들여 출력하는 비교 제어부, 및 상기 비교 제어부로부터 출력된 제 1 보안키를 상기 제 2 보안키 저장부에서 읽어들인 제 2 보안키와 비교하여 상기 보안키 비교 신호를 출력하는 비교부를 포함하여 구성될 수도 있다.

여기에서, 상기 비교 로직부는 상기 제 1 보안키와 상기 제 2 보안키가 동일한 경우에는 '로우'인 보안키 비교 신호를 출력하고, 상기 제 1 보안키와 상기 제 2 보안키가 상이한 경우에는 '하이'인 보안키 비교 신호를 출력하도록 구성될 수 있다.

여기에서, 상기 억세스 제어부는 상기 비교 로직부로부터 상기 보안키 비교 신호를 수신하고, 상기 외부 입출력 핀으로부터 상기 테스트 인에이블 신호를 수신하여 논리 연산한 억세스 선택 신호를 출력하는 논리 연산부, 및 상기 억세스 선택 신호에 응답하여, 상기 외부 입출력 핀을 통하여 수신한 상기 온 칩 메모리부에 대한 억세스 신호의 상기 온 칩 메모리부로의 전달 여부를 결정하는 인터페이스부를 포함하여 구성될 수 있다.

이 경우에, 상기 논리 연산부는 상기 보안키 비교 신호가 상기 제 1 보안키와 상기 제 2 보안키가 상이함을 지시하고, 상기 테스트 인에이블 신호가 활성화되었을 때, 활성화된 억세스 선택 신호를 출력하는 논리 연산 소자를 포함하여 구성될 수 있다.

이 경우에, 상기 인터페이스부는 상기 억세스 선택 신호에 응답하여, 상기 메모리 컨트롤러에서 발생된 상기 온 칩 메모리부에 대한 억세스 신호와 상기 외부 입출력 핀을 통하여 수신한 상기 온 칩 메모리부에 대한 억세스 신호를 선택적으로 상기 온 칩 메모리부에 전달하는 다중화 로직을 포함하여 구성될 수 있다.

여기에서, 상기 메모리 컨트롤러는, 상기 제 1 보안키를 상기 온 칩 메모리부의 상기 소정 영역에서 읽어들여 상기 비교 로직부에 전달하는 중에는 비활성화되고, 모두 전달했을 경우에는 활성화되는 로드 완료 신호를 상기 억세스 제어부로 출력하도록 구성될 수 있다.

이 경우에, 상기 억세스 제어부는 상기 비교 로직부로부터 상기 보안키 비교 신호를 수신하고, 상기 외부 입출력 핀으로부터 상기 테스트 인에이블 신호를 수신하고, 상기 메모리 컨트롤러로부터 상기 로드 완료 신호를 수신하여 논리 연산한 억세스 선택 신호를 출력하는 논리 연산부, 및 상기 억세스 선택 신호에 응답하여, 상기 외부 입출력 핀을 통하여 수신한 상기 온 칩 메모리부에 대한 억세스 신호의 상기 온 칩 메모리부로의 전달 여부를 결정하는 인터페이스부를 포함하여 구성될 수 있다.

이 경우에, 상기 논리 연산부는 상기 보안키 비교 신호가 상기 제 1 보안키와 상기 제 2 보안키가 상이함을 지시하고, 상기 테스트 인에이블 신호가 활성화되었으며, 상기 로드 완료 신호가 활성화되었을 때, 활성화된 억세스 선택 신호를 출력하는 논리 연산 소자를 포함하여 구성될 수 있다.

이 경우에, 상기 인터페이스부는 상기 억세스 선택 신호에 응답하여, 상기 메모리 컨트롤러에서 발생된 상기 온 칩 메모리부에 대한 억세스 신호와 상기 외부 입출력 핀을 통하여 수신한 상기 온 칩 메모리부에 대한 억세스 신호를 선택적으로 상기 온 칩 메모리부에 전달하는 다중화 로직을 포함하여 구성될 수 있다.

여기에서, 상기 온 칩 메모리부는 비휘발성 멀티-타임 프로그래머블 메모리 셀 어레이로 구성될 수 있고, 상기 비휘발성 멀티-타임 프로그래머블 메모리 셀 어레이로는 플래쉬 메모리 셀 어레이가 이용될 수 있다.

여기에서, 상기 제 2 보안키 저장부는 하드 와이어드 방식 또는 마스크 롬을 이용하여 구현될 수 있다.

상기 목적을 달성하기 위해 본 발명의 다른 형태는, 제 1 보안키와 제 2 보안키를 소정 영역에 저장하는 온 칩 메모리부, 칩 내부로부터 상기 온 칩 메모리부에 대한 억세스 신호를 발생시키는 메모리 컨트롤러, 칩 외부로부터 상기 온 칩 메모리부에 대한 억세스를 요청하기 위한 테스트 인에이블 신호와 상기 온 칩 메모리부에 대한 억세스 신호를 수신하는 외부 입출력 핀, 상기 온 칩 메모리부로부터 상기 메모리 컨트롤러를 통하여 상기 제 1 보안키와 상기 제 2 보안키를 읽어들여 비교

하고 보안키 비교 신호를 출력하는 비교 로직부, 및 상기 보안키 비교 신호에 응답하여, 상기 외부 입출력 핀을 통하여 수신된 상기 온 칩 메모리부에 대한 억세스 신호의 허용 여부를 결정하는 억세스 제어부를 포함한 것을 특징으로 하는 온 칩 메모리를 이용한 기밀 정보 보안 장치를 제공한다.

여기에서, 상기 비교 로직부는 상기 메모리 컨트롤러를 통하여, 상기 온 칩 메모리부의 상기 소정 영역에 기록된 제 1 보안키를 읽어들여 저장하고 출력하는 제 1 레지스터부, 상기 온 칩 메모리부의 상기 소정 영역에 기록된 제 2 보안키를 읽어들여 저장하고 출력하는 제 2 레지스터부, 및 상기 제 1 레지스터부로부터 출력된 제 1 보안키를 상기 제 2 레지스터부로부터 출력된 제 2 보안키와 비교하여 상기 보안키 비교 신호를 출력하는 비교부를 포함하여 구성될 수 있다.

이 경우에, 상기 제 1 레지스터부와 상기 제 2 레지스터부 중의 적어도 하나는 적어도 하나의 비트에 연결된 퓨즈를 포함하고, 상기 퓨즈는 상기 퓨즈가 연결된 비트의 상태를 '0' 또는 '1'로 고정시키는 역할을 수행하도록 구성될 수도 있다.

여기에서, 상기 메모리 컨트롤러는 상기 제 1 보안키와 상기 제 2 보안키를 상기 온 칩 메모리부의 상기 소정 영역에서 읽어들여 상기 비교 로직부에 전달하는 중에는 비활성화되고, 모두 전달했을 경우에는 활성화되는 로드 완료 신호를 상기 억세스 제어부로 출력하도록 구성될 수 있다.

상기 다른 목적을 달성하기 위해 본 발명은, 제 1 보안키와 제 2 보안키를 비교하는 보안키 비교 단계, 칩 외부로부터 온 칩 메모리부에 대한 억세스 요청을 수신하는 단계, 상기 제 1 보안키와 상기 제 2 보안키가 동일한 경우에는 상기 억세스 요청을 차단하는 단계, 및 상기 제 1 보안키와 상기 제 2 보안키가 상이한 경우에는 상기 억세스 요청에 응답하여 상기 온 칩 메모리부에 대한 억세스를 수행하는 단계를 포함한 온 칩 메모리 장치를 이용한 기밀 정보 보안 방법을 제공한다.

여기에서, 상기 온 칩 메모리부에 대한 억세스를 수행하는 단계는 상기 제 1 보안키를 상기 온 칩 메모리부의 소정 영역에 읽거나 쓰는 동작을 수행할 수 있다. 마찬가지로, 상기 온 칩 메모리부에 대한 억세스를 수행하는 단계는 상기 제 2 보안키를 상기 온 칩 메모리부의 소정 영역에 읽거나 쓰는 동작을 수행할 수도 있다.

여기에서, 상기 기밀 정보 보안 방법은 상기 보안키 비교 단계의 진행 중에는 상기 칩 외부로부터 온 칩 메모리부에 대한 억세스 요청을 차단하는 단계를 추가로 포함할 수 있다.

여기에서, 상기 보안키 비교 단계는 상기 제 1 보안키와 상기 제 2 보안키가 동일한 경우에는 비활성화된 보안키 비교 신호를 출력하고, 상기 제 1 보안키와 상기 제 2 보안키가 상이한 경우에는 활성화된 보안키 비교 신호를 출력하도록 구성될 수 있다.

이 경우에, 상기 억세스 요청을 차단하는 단계와 상기 억세스 요청에 응답하여 상기 온 칩 메모리부에 대한 억세스를 수행하는 단계는 상기 보안키 비교 신호에 응답하여 이루어질 수 있다.

이 경우에, 상기 보안키 비교 단계는 상기 온 칩 메모리 장치를 이용한 기밀 정보 보안 방법이 수행되는 칩이 파워 온 되거나, 리셋될 때마다 이루어질 수 있다.

이 경우에, 상기 보안키 비교 신호는 상기 칩이 다시 파워 다운되거나, 리셋될 때까지 상태가 유지되도록 구성될 수 있다.

이하, 본 발명에 따른 바람직한 실시예를 첨부된 도면을 참조하여 상세하게 설명한다. 이 실시예는 당해 기술 분야에서 통상의 지식을 가진 자들이 본 발명을 실시할 수 있게 충분히 상세하게 기술한다.

제 1 실시예

도2는 본 발명에 따른 기밀 정보 보안 장치의 블록도이다.

도2를 참조하면, 본 발명에 따른 온 칩 메모리 장치를 이용한 기밀 정보 보안 장치(200)는 온 칩 메모리부(201), 메모리 컨트롤러(202), 비교 로직부(203), 제 2 보안키 저장부(204), 외부 입출력 핀(205) 및 억세스 제어부(206)를 포함하여 구성될 수 있다.

온 칩 메모리부(201)로는 비휘발성이고 재프로그래밍이 가능한 플래쉬 메모리 셀 어레이(flash memory cell array)가 널리 사용될 수 있다. 플래쉬 메모리 셀 어레이를 대체할 수 있는 비휘발성 특성과 재프로그래밍이 가능한 특성을 가지는 메

모리 어레이는 무엇이든 상기 온 칩 메모리부(201)로 이용될 수 있음은 당업자에게 있어 자명하다. 예를 들면, 강유전체 메모리(FRAM; Ferroelectric RAM), 강자성 메모리(MRAM; Magnetic RAM) 및 상변화 메모리(PRAM; Phase Change RAM) 등의 차세대 메모리 셀 어레이들이 이용될 수 있다.

온 칩 메모리부(201)에는 인증키를 포함한 기밀 정보가 기록되고, 소정의 영역(211)에는 기록된 기밀 정보에 대한 외부 접근을 제한하기 위해서 이용되는 제 1 보안키(SEC1KEY)가 기록된다.

메모리 컨트롤러(202)는 내부적으로 온 칩 메모리부(201)에 대한 입출력을 제어하는 장치로서, 상기 온 칩 메모리부(202)로서 선택되는 메모리 셀 어레이의 종류에 대응하여 메모리 컨트롤러(202)는 구성된다. 한편, 외부에서의 메모리 컨트롤러(202)를 통한 온 칩 메모리부(201)에 대한 억세스는 어드레스(address) 단위의 접근이 아니라, 정보(information) 단위로 접근이 가능하도록 구성되어지는 것이 일반적이다. 온 칩 메모리부(201)에 기록된 기밀 정보들에 사용자가 메모리 컨트롤러(202)를 통하여 간접적으로 접근하는 것을 방지하기 위한 목적이다. 예컨대, 메모리 컨트롤러(202)를 통하여 온 칩 메모리부(201)에 기록된 기밀 정보들에 억세스하는 내부 회로들은 기밀 정보를 어드레스 단위로 지정하여 억세스할 수 없고, 정보 단위로 요청하는 방식으로 동작한다.

제 2 보안키 저장부(204)는 기밀 정보 보안 장치(200)가 구현된 칩(chip)의 내부에 존재하는 구성요소로서, 온 칩 메모리부(201)의 소정 영역(211)에 기록되는 제 1 보안키(SEC1KEY)와 비교되는 제 2 보안키(SEC2KEY)를 저장하기 위한 구성요소이다.

제 2 보안키 저장부(204)는 하드 와이어드(hard-wired) 방식을 이용하여 제 2 보안키(SEC2KEY)를 저장하도록 구현될 수도 있고, 별도의 온 칩 읽기 전용 메모리 장치, 예컨대 마스크 롬을 이용하여 구성될 수도 있다. 이후에 상술되겠으나, 제 1 보안키(SEC1KEY) 및 제 2 보안키(SEC2KEY)는 장치별로 상이하게 구성될 필요는 없기 때문에, 언급된 바와 같이 하드 와이어드 방식이나, 마스크 롬을 이용하여 저장될 수 있다.

외부 입출력 핀(205)은 테스트 인에이블 신호(TEST_EN)를 입력받기 위한 핀(TEST_EN_PIN)과 온 칩 메모리부(101)를 억세스하기 위한 어드레스 신호(E_ADDR)를 입력받는 어드레스 신호 핀(E_ADDR_PIN), 제어 신호(E_CTRL)를 입력받는 제어 신호 핀(E_CTRL_PIN), 및 데이터 신호(E_DIO)를 입출력하는 데이터 신호 핀(E_DIO_PIN)들로 구성된다. 외부 입출력 핀(205)의 역할은 제품의 생산 과정에서 온 칩 메모리부(201)에 인증키 등의 기밀 정보를 기입하거나 변경하는 것이 가능하도록 하기 위한 것임은 도1에서 예시한 종래 기술의 기밀 정보 보안 장치와 동일하다.

비교 로직부(203)는 온 칩 메모리부(201)의 소정 영역(211)에 기록된 제 1 보안키(SEC1KEY)와 제 2 보안키 저장부(204)에 기록된 제 2 보안키(SEC2KEY)를 서로 비교하여 보안키 비교 신호(COMPARE_RES)를 출력하는 구성요소이다.

비교 로직부(203)는 온 칩 메모리부(201)의 소정 영역(211)에 기록된 제 1 보안키(SEC1KEY)와 제 2 보안키 저장부(204)에 기록된 제 2 보안키(SEC2KEY)가 동일할 경우에는 '로우'로 비활성화된 보안키 비교 신호(COMPARE_RES)를 출력하고, 두 개의 보안키가 상이할 경우에는 '하이'로 활성화된 보안키 비교 신호(COMPARE_RES)를 출력하도록 구성될 수 있다. 비교 로직부(203)의 자세한 구성에 대해서는 후술된다.

억세스 제어부(206)는 상기 외부 입출력 핀(205)들 중 테스트 인에이블 핀(TEST_EN_PIN)을 통하여 입력된 테스트 인에이블 신호(TEST_EN)와 상기 비교 로직부(203)가 출력한 보안키 비교 신호(COMPARE_RES)에 응답하여, 외부로부터의 온 칩 메모리부(201)에 대한 억세스를 제어하는 역할을 수행하는 구성요소이다.

억세스 제어부(206)는 활성화된 테스트 인에이블 신호(TEST_EN)가 입력되고, 보안키 비교 신호(COMPARE_RES)가 활성화된 경우에는 외부 입출력 핀(205)들을 통하여 수신한 외부로부터의 억세스 신호(E_ADDR,E_CTRL,E_DIO)를 온 칩 메모리부(201)로 전달한다.

반대로, 억세스 제어부(206)는 비활성화된 테스트 인에이블 신호(TEST_EN)가 입력되는 경우와 활성화된 테스트 인에이블 신호(TEST_EN)와 비활성화된 보안키 비교 신호(COMPARE_RES)가 입력되는 경우에는 외부 입출력 핀(205)들을 통하여 수신한 외부로부터의 억세스 신호(E_ADDR,E_CTRL,E_DIO)를 차단하고, 메모리 컨트롤러(202)의 억세스 신호(I_ADDR,I_CTRL,I_DIO)만을 온 칩 메모리부(201)에 전달한다.

억세스 제어부(206)의 자세한 구성에 대해서는 후술된다.

본 발명에 따른 기밀 정보 보안 장치(200)는 온 칩 메모리부(201)에 기록되는 제 1 보안키(SEC1KEY)와 제 2 보안키 저장부(204)에 기록되는 제 2 보안키(SEC2KEY)의 비교를 통해서 외부로부터의 온 칩 메모리부(201)에 대한 접근의 허용과 차단 여부를 결정하는 방식으로 동작한다. 따라서, 기밀 정보 보안 장치(200)를 이용한 기밀 정보의 기록 및 변경과, 기밀 정보의 보안 절차는 다음과 같이 정리된다.

먼저, 제품의 생산 과정에서는, 온 칩 메모리부(201)에 인증키를 포함한 기밀 정보를 기록하기 위해서 외부 입출력 핀(205)들을 이용하여 활성화된 테스트 인에이블 신호(TEST_EN)를 입력하고, 온 칩 메모리부(201)에 대한 억세스 신호(E_ADDR, E_CTRL, E_DIO)들을 입력한다.

비교 로직부(203)는 온 칩 메모리부(201)의 소정 영역(211)에서 제 1 보안키(SEC1KEY)의 내용을 읽어들이고, 제 2 보안키 저장부(204)로부터 제 2 보안키(SEC2KEY)를 읽어들여 두 개의 보안키의 내용을 비교하고 그 결과를 보안키 비교 신호(COMPARE_RES)로서 출력한다. 이때, 제 1 보안키(SEC1KEY)는 아직 기록되어지지 않은 상태여서 이미 기록되어 있는 제 2 보안키(SEC2KEY)와는 상이하므로, '하이'로 활성화된 보안키 비교 신호(COMPARE_RES)가 출력된다.

억세스 제어부(206)는 보안키 비교 신호(COMPARE_RES)와 테스트 인에이블 신호(TEST_EN)가 활성화되어 있으므로, 외부 입출력 핀(205)들을 통해 입력된 온 칩 메모리부(201)에 대한 억세스 신호(E_ADDR, E_CTRL, E_DIO)들을 온 칩 메모리부(201)에 전달한다. 따라서, 온 칩 메모리부(201)에는 외부로부터의 억세스 요청에 응답하여 인증키를 포함한 기밀 정보가 기록되거나 및 변경될 수 있다.

온 칩 메모리부(201)에 인증키를 포함한 기밀 정보의 기록이 완료되면, 소정의 영역(211)에 제 1 보안키(SEC1KEY)를 기록한다. 제 1 보안키(SEC1KEY)는 제 2 보안키(SEC2KEY)와 동일한 길이와 내용을 가진 비트열로 구성된다.

다음으로, 본 발명의 기밀 정보 보안 장치(200)가 다시 파워 온(power-on)되거나 리셋(reset)되면, 예컨대, 메모리 컨트롤러(202)가 리셋 신호(RESET)를 수신하면, 비교 로직부(203)는 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)를 다시 읽어들여 두 개의 보안키의 내용을 비교하고 그 결과를 보안키 비교 신호(COMPARE_RES)로서 출력한다. 이때에는 앞선 기밀 정보 기록 단계에서 제 2 보안키(SEC2KEY)와 동일한 제 1 보안키(SEC1KEY)가 온 칩 메모리부(201)의 소정 영역(211)에 이미 기록된 상태이므로 보안키 비교 신호(COMPARE_RES)는 '로우'로 비활성화된다.

억세스 제어부(206)는 보안키 비교 신호(COMPARE_RES)가 비활성화되어 있으므로, 활성화된 테스트 인에이블 신호(TEST_EN)가 입력된다 할지라도, 외부 입출력 핀(205)들을 통해 입력된 온 칩 메모리부(201)에 대한 억세스 신호(E_ADDR, E_CTRL, E_DIO)의 온 칩 메모리부(201)로의 전달을 차단한다. 따라서, 온 칩 메모리부(201)에 대한 더 이상의 외부로부터의 기록 및 변경은 원천적으로 차단되어 온 칩 메모리부(201)에 기록된 인증키를 포함한 기밀 정보의 유출 및 파괴를 막을 수 있다.

한편, 상기 본 발명의 기밀 정보 보안 장치(200)에 이용되는 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)는 가급적 긴 길이를 가지는 비트열로 구성되고, 복잡한 패턴을 가지는 것이 바람직하다. 상기 언급한 바와 같이, 온 칩 메모리부(201)로서 사용될 수 있는 플래쉬 메모리 셀 어레이를 구성하는 모든 셀들은 최초 상태에서 공정에 따라서 '0' 또는 '1'의 상태를 유지하고 있게되는 것이 일반적이다. 그러나, 우연히 특정 셀들의 상태가 다르게 유지된다면, 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)가 우연적으로 일치되는 경우가 발생하여 외부 입출력 핀(205)을 통한 온 칩 메모리부(201)에 대한 기록 및 변경이 최초부터 불가능해지는 경우가 발생될 수 있기 때문이다.

도3은 본 발명의 기밀 정보 보안 장치에 이용되는 비교 로직부의 한 구성예를 도시한 블록도이다.

도3을 참조하면, 도2에서 예시한 본 발명의 기밀 정보 보안 장치에 이용될 수 있는 비교 로직부의 한 구성예를 알 수 있다.

도3의 비교 로직부(203)는 레지스터부(301)와 비교부(302)를 포함하여 구성될 수 있다. 레지스터부(301)는 메모리 컨트롤러(202)를 통하여 상기 온 칩 메모리 부(201)의 소정 영역(211)에서 제 1 보안키(SEC1KEY)를 읽어와서 저장하는 역할을 수행한다.

상기 레지스터부(301)의 필요성은 비교부(302)의 구성에 따라서 달라질 수 있다. 도3의 비교 로직부(203)는 레지스터부(301)에 제 1 보안키(SEC1KEY)의 내용을 모두 옮기고, 제 2 보안키 저장부(204)로부터 순차적으로 제 2 보안키(SEC2KEY)를 읽어와서 비교부(302)에서 비교하는 방식으로 동작한다. 이 경우에, 레지스터부(301)는 상기 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)의 길이 만큼의 비트열을 저장할 수 있도록 구성된다.

비교부(302)는 상기한 바와 같이, 레지스터부(301)로부터 입력되는 제 1 보안키(SEC1KEY)와 제 2 보안키 저장부(204)로부터 입력되는 제 2 보안키(SEC2KEY)를 서로 비교한다. 따라서, 비교부(302)는 적어도 하나의 비교기(comparator; 303)를 포함하여 구성될 수 있고, 상기 레지스터부(301)와 제 2 보안키 저장부(204)의 구성에 따라서 비교기의 숫자 및 연결 구성이 다양하게 이루어질 수 있다.

예를 들면, 쉬프트 레지스터(shift-register)로 구성된 레지스터부(301)와 제 2 보안키 저장부(204)로부터 순차적으로 1비트씩의 정보를 입력받아서 1비트씩을 서로 비교하는 구성이 가능하다.

비교부(302)는 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)의 비교결과로서 보안키 비교 신호(COMPARE_RES)를 출력한다. 도3의 비교부 구성을 예를 들면, 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)의 모든 비트가 동일하면 보안키 비교 신호(COMPARE_RES)는 '0'을 유지하고, 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)가 한 비트라도 상이하면 보안키 비교 신호(COMPARE_RES)는 '1'로 출력된다.

한편, 기밀 정보 보안 장치(200)가 파워 온 되거나, 리셋된 경우에는 비교 로직부(203)가 온 칩 메모리부(201)에 기록된 제 1 보안키(SEC1KEY)와 제 2 보안키 저장부(204)에 기록된 제 2 보안키(SEC2KEY)를 비교하여 보안키 비교 신호(COMPARE_RES)를 출력하기까지의 여유시간이 필요하다.

상기 비교를 위한 보안키의 로드(load) 시간 동안의 오동작을 방지하기 위하여, 메모리 컨트롤러(202)는 리셋 신호를 수신하였을 때, 비교 로직부(203)에 대하여 온 칩 메모리부(201)에 기록된 제 1 보안키(SEC1KEY)를 전달하는 중에는 로드 완료 신호(LOAD)를 '로우'로 비활성화 상태로 유지한다. 비교 로직부(203)에 대한 제 1 보안키(SEC1KEY)의 로딩(loading)이 완료되면, 메모리 컨트롤러(202)는 로드 완료 신호(LOAD)를 '하이'로 활성화 상태로 변경한다.

로드 완료 신호(LOAD)는 억세스 제어부(206)에 입력되어 칩 외부로부터의 억세스 요청을 온 칩 메모리부(201)로 전달할 것인지를 결정하는 신호로서 이용되며, 자세한 동작은 후술된다.

한편, 상기 도3과 같은 비교 로직부의 구성에 있어서, 제 1 보안키(SEC1KEY)를 읽어들여 저장하는 레지스터부(301)의 구성을 생략하여 보다 단순화한 비교 로직부의 구성도 가능할 수 있다.

이 경우에, 상기 비교 로직부는 메모리 컨트롤러(202)로부터 온 칩 메모리부(201)의 소정 영역(211)에 저장된 제 1 보안키(SEC1KEY)를 비트 단위 또는 바이트 단위로 읽어들여 순차적으로 비교부(302)의 비교기(303)로 전달하기 위한 제어 로직을 포함하여야 한다.

도4는 본 발명의 기밀 정보 보안 장치에 이용되는 비교 로직부의 다른 구성예를 도시한 블록도이다.

도4를 참조하면, 도2에서 예시한 본 발명의 기밀 정보 보안 장치에 이용될 수 있는 비교 로직부의 다른 구성예를 알 수 있다.

도4에서 예시하고 있는 비교 로직부(203)는 비교부(302)와 비교 제어부(304)를 포함하여 구성될 수 있다. 도3에서 예시한 비교 로직부와 비교하면, 레지스터부(301)가 생략되고, 비교 제어부(304)가 레지스터부(301)를 대체하여 구성된다.

상기 비교 제어부(304)는 제 2 보안키 저장부(204)로부터 제 2 보안키(SEC2KEY)가 읽어들여지는 단위(예컨대, 비트 또는 바이트)에 동기적으로 제 1 보안키(SEC1KEY)를 메모리 컨트롤러(202)를 통하여 온 칩 메모리부(201)로부터 읽어들여 비교부(302)의 비교기(303)에 전달하기 위한 역할을 수행한다.

한편, 비교부(302) 및 비교기(303)를 포함한 나머지 구성 요소들의 동작 및 구성은 도3에서 예시한 비교 로직부의 대응되는 구성 요소들과 동일하므로 설명은 생략된다.

본질적으로, 도3에서 예시한 비교 로직부와 도4에서 예시한 비교 로직부의 구성은 동일한 기능을 수행하기 위한 다른 구성으로, 당업자에게 있어서, 상기 도3 및 도4를 제외한 다양한 비교 로직부의 구성이 가능함은 자명하다.

도5는 본 발명의 기밀 정보 보안 장치에 이용되는 비교 로직부의 레지스터부 동작을 예시한 흐름도이다.

도5를 참조하면, 도3에서 본 발명의 기밀 정보 보안 장치에 이용될 수 있는 비교 로직부의 레지스터부(301)의 동작이 설명된다.

시스템이 파워 온 되거나 리셋되어 메모리 컨트롤러(202)가 리셋 신호(RESET)를 수신하면, 비교 로직부의 레지스터부(301)로의 제 1 보안키(SEC1KEY) 로딩이 시작된다(S51).

먼저, 리셋 신호(RESET)를 수신한 메모리 컨트롤러(202)는 로드 완료 신호(LOAD)를 '로우'로 비활성화시킨다. 로드 완료 신호(LOAD)는 억세스 제어부(206)에 입력되어, 칩 외부로부터의 억세스 요청을 온 칩 메모리부(201)로 전달할 것인지를 결정하는 신호로서 이용된다.

다음으로, 온 칩 메모리부(201)로부터 제 1 보안키(SEC1KEY)를 읽어들여 레지스터부(301)로 옮기는 단계(S53)가 진행된다.

레지스터부(301)의 구성과 온 칩 메모리부(201)를 구성하는 메모리 셀 어레이의 특성에 따라서 달라질 수 있으나, 도5에서는 8비트 단위로 온 칩 메모리부(201)의 소정 영역(211)에서 제 1 보안키(SEC1KEY)를 읽어들여 8비트 단위로 구성된 레지스터부(301)에 저장하는 과정을 예시하고 있다. 예컨대, 제 1 보안키(SEC1KEY)가 32비트 길이를 가진다면, 4번의 리드 사이클(read cycle)만에 제 1 보안키가 레지스터부(301)에 로드된다.

온 칩 메모리부(201)로부터 레지스터부(301)로의 제 1 보안키(SEC1KEY)의 로딩이 완료되면, 메모리 컨트롤러(202)는 로드 완료 신호(LOAD)를 '하이'로 활성화시켜 억세스 제어부(206)로 전달하면서(S54), 비교 로직부(203)의 제 1 보안키(SEC1KEY) 로딩 동작이 완료된다(S55).

도6은 본 발명의 기밀 정보 보안 장치에 이용되는 억세스 제어부의 구성예를 도시한 블록도이다.

도6을 참조하면, 도2에서 예시한 본 발명의 기밀 정보 보안 장치에 이용될 수 있는 억세스 제어부의 구성예를 알 수 있다.

도6을 참조하면, 본 발명의 기밀 정보 보안 장치(200)를 구성하는 억세스 제어부(206)는 논리 연산부(601) 및 인터페이스부(604)를 포함하여 구성될 수 있다. 논리 연산부(601)는 온 칩 메모리부(201)에 대한 칩 외부로부터의 억세스 요청을 허용할 것인지를 결정하기 위한 논리 소자들(602,603)을 포함하여 구성될 수 있다.

자세하게는, 논리 연산부(601)는 비교 로직부(203)로부터 출력된 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)를 비교한 결과인 보안키 비교 신호(COMPARE_RES)와 외부 입출력 핀(205)에서 수신한 테스트 인에이블 신호(TEST_EN)를 논리곱(AND)하는 논리곱 소자(602)를 포함한다.

또한, 논리 연산부(601)는 논리곱 소자(602)로부터 출력된 결과값과 메모리 컨트롤러(202)로부터 출력된 로드 완료 신호(LOAD)를 수신하여 논리곱하는 논리곱 소자(603)를 포함한다.

따라서, 논리 연산부(601)는 하기 표1과 같은 관계에 의하여 칩 외부로부터의 온 칩 메모리부(201)에 대한 억세스 허용 여부를 결정하는 억세스 선택 신호(SEL)를 인터페이스부(604)로 출력하게 된다.

[표 1]

case	LOAD	COMPARE_RES	TEST_EN	억세스 허용여부 (SEL)
1	0	0	0	X
2	0	0	1	X
3	0	1	0	X
4	0	1	1	X
5	0	0	0	X
6	0	0	1	X
7	0	1	0	X
8	0	1	1	0

먼저, 메모리 컨트롤러(202)에 의해서 온 칩 메모리부(201)의 소정 영역(211)에 기록된 제 1 보안키(SEC1KEY)가 비교 로직부(203)로 완전히 로드되지 않은 상태에서는, 로드 완료 신호(LOAD)는 '0'으로 유지된다. 시스템의 파워 온이나 리셋 시에 보안키의 비교 결과가 도출되지 않은 상태에서 테스트 인에이블 신호(TEST_EN)에 의해 칩 외부의 억세스 요청이 허용되는 것을 방지하기 위해서, 로드 완료 신호(LOAD)가 '0'으로 유지된 상태에서는 칩 외부의 억세스 요청은 원천적으로 차단된다.

메모리 컨트롤러(202)에 의해서 온 칩 메모리부(201)의 소정 영역(211)에 기록된 제 1 보안키(SEC1KEY)가 비교 로직부(203)로 완전히 로드되어, 로드 완료 신호(LOAD)가 '1'로 유지되면, 외부로부터의 억세스 요청은 보안키 비교 신호(COMPARE_RES)에 응답하여 허용 여부가 결정된다.

도3 및 도4를 통하여 설명된 비교 로직부(203)의 구성에 의하면, 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)가 동일한 값을 유지한 상태에서 보안키 비교 신호(COMPARE_RES)는 '0'으로 출력된다. 반대로, 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)가 상이한 값인 경우에는 보안키 비교 신호(COMPARE_RES)는 '1'로 출력된다.

인터페이스부(604)는 논리 연산부(601)가 출력한 억세스 선택 신호(SEL)에 응답하여, 칩 내외부의 억세스 요청을 선택적으로 온 칩 메모리부(201)에 전달하기 위한 구성요소이다.

도6을 참조하면, 인터페이스부(604)는 메모리 컨트롤러(202)로부터의 억세스 신호(INT_DIO, INT_ADDR, INT_CTRL)와 칩외부로부터 수신된 억세스 신호(EXT_DIO, EXT_ADDR, EXT_CTRL)를 입력받고, 억세스 선택 신호(SEL)에 응답하여 선택적으로 억세스 요청을 온 칩 메모리부(201)로 전달한다. 따라서, 인터페이스부(604)는 소정의 다중화 로직(multiplexing login)을 포함하여 구성될 수 있음은 당업자에게 있어 자명하다.

예컨대, 인터페이스부(604)는 비활성화된 억세스 선택 신호(SEL)를 입력받은 경우에는, 메모리 컨트롤러(202)로부터의 억세스 신호(INT_DIO, INT_ADDR, INT_CTRL)를 온 칩 메모리부(201)로 전달한다.

반대로, 인터페이스부(604)는 활성화된 억세스 선택 신호(SEL)를 입력받은 경우에는, 외부 입출력 핀(205)을 통하여 칩 외부로부터 수신된 억세스 신호(EXT_DIO, EXT_ADDR, EXT_CTRL)를 온 칩 메모리부(201)로 전달한다.

한편, 인터페이스부(604)는, 상기 온 칩 메모리부(201)가 듀얼 포트(dual port) 구성을 취하고 있는 경우에는 다른 구성을 취할 수 있다.

즉, 온 칩 메모리부(201)가 상기 메모리 컨트롤러(202)와 외부 입출력 핀(205)으로부터의 억세스 신호를 개별적으로 입력받을 수 있는 두 개의 포트를 구비하고 있는 경우에는, 인터페이스부(604)의 다중화 로직은 생략될 수 있다.

따라서, 메모리 컨트롤러(202)로부터의 억세스 신호(I_ADDR, I_CTRL, I_DIO)는 직접적으로 온 칩 메모리부(201)의 제 1 포트에 연결되고, 외부 입출력 핀(205)으로부터의 억세스 신호(E_ADDR, E_CTRL, E_DIO)는 논리 연산부(601)가 출력한 억세스 선택 신호(SEL)에 응답하여 온 칩 메모리부(201)의 제 2 포트를 통하여 입력되거나 차단되는 방식으로 인터페이스부(604)는 구성될 수도 있다.

도7은 본 발명의 기밀 정보 보안 방법의 전체적인 흐름도이다.

도7을 참조하면, 본 발명의 기밀 정보 보안 방법의 전체적인 동작을 알 수 있다. 특히, 도7에서 예시한 흐름도는 도2에서 예시한 기밀 정보 보안 장치(200)를 기준으로 하여 구성한 것이지만, 도7에서 예시하고 있는 기밀 정보 보안 방법은 본 발명에 따른 기밀 정보 보안 장치의 다른 구성에도 적용될 수 있음은 자명하다.

메인 칩이 파워 온 되거나 리셋되면 본 발명의 기밀 정보 보안 방법이 시작된다(S71).

온 칩 메모리부(201)의 소정 영역(211)에 기록된 제 1 보안키(SEC1KEY)와 제 2 보안키 저장부(204)에 기록된 제 2 보안키(SEC2KEY)가 서로 비교된다(S72). 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)의 비교는 기밀 정보 보안 장치(200)의 비교 로직부(203)에서 이루어지는 동작으로, 비교 로직부(203)의 구성에 따라서, 다르게 이루어질 수 있음은 도3 및 도4를 통하여 이미 설명된 바와 같다.

한편, 상기 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)를 비교하는 단계에서 메모리 컨트롤러(202)를 통하여 온 칩 메모리부(201)에 기록된 제 1 보안키(SEC1KEY)를 읽어들이는 동안에는 칩 외부로부터의 억세스 신호를 원천적으로 차단하는 과정이 추가적으로 요구될 수 있다.

제 1 보안키(SEC1KEY)를 온 칩 메모리부(201)로부터 비교 로직부(203)로 로드하기 위한 절차와 제 1 보안키(SEC1KEY)의 로드 진행 중에 억세스 신호의 원천적인 차단 절차는 상기 도5에서 예시한 흐름도에 의해 이루어질 수 있음은 이미 설명된 바와 같다.

다음으로, 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)가 동일한지 여부를 판단한다(S73). 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)가 동일한 경우에는 비교 로직부(203)가 출력하는 보안키 비교 신호(COMPARE_RES)는 '0'으로 유지된다(S74_1). 반대로 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)가 상이한 경우에는 비교 로직부(203)가 출력하는 보안키 비교 신호(COMPARE_RES)는 '1'로 유지된다(S74_2).

칩 외부로부터 활성화된 테스트 인에이블 신호(TEST_EN)와 억세스 신호(E_ADDR, E_CTRL, E_DIO)를 수신하면 칩 외부로부터의 억세스 신호의 허용 여부를 판단하는 절차가 진행된다(S75).

테스트 인에이블 신호(TEST_EN)가 활성화된 상태에서 보안키 비교 신호(COMPARE_RES)의 상태를 판단한다(S76).

보안키 비교 신호(COMPARE_RES)가 '0' 상태이면, 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)가 동일한 경우이므로 이미 제 2 보안키(SEC2KEY)와 동일한 제 1 보안키(SEC1KEY)가 온 칩 메모리부(201)의 소정 영역(211)에 기록된 상태임을 의미한다. 따라서, 칩 외부로부터의 억세스 신호는 차단된다(S77).

반대로, 보안키 비교 신호(COMPARE_RES)가 '1' 상태이면, 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)가 상이한 경우이므로 아직 제 2 보안키(SEC2KEY)와 동일한 제 1 보안키(SEC1KEY)가 온 칩 메모리부(201)의 소정 영역(211)에 기록되지 않은 상태임을 의미한다. 따라서, 칩 외부로부터의 억세스 신호(E_ADDR, E_CTRL, E_DIO)는 온 칩 메모리부(201)에 전달된다(S78). 따라서, 상기 억세스 신호에 의해서 온 칩 메모리부(201)에는 인증키를 포함한 기밀 정보가 기록 또는 검증될 수 있다.

최종적으로 보안키 비교 신호(COMPARE_RES)가 '1'인 상태에서, 기밀 정보의 기록이 완료되면, 온 칩 메모리부(201)의 소정 영역(211)에 제 1 보안키(SEC1KEY)를 기록한다(S79).

마지막으로, 시스템이 파워 다운(power down)되거나, 시스템 리셋 신호가 인가되면 온 칩 메모리부(201)에 대한 외부로부터의 더 이상의 억세스는 차단된다(S80).

제 2 실시예

상기 제 1 실시예에서는 제 2 보안키(SEC2KEY)는 제 2 보안키 저장부(204)에 별도로 저장된다. 제 2 보안키 저장부(204)는 하드 와이어드 방식 또는 칩 내부에 구현된 마스크 롬 등으로 온 칩 메모리부(201)와는 별도로 구성되어야 함은 이미 언급된 바와 같다.

그러나, 제 1 보안키(SEC1KEY)와 마찬가지로, 제 2 보안키(SEC2KEY) 역시 온 칩 메모리부(201)에 저장하는 기밀 정보 보안 장치(200)의 다른 구성도 가능하다. 이와 같은 구성의 경우, 기록된 정보가 쉽게 유출되지 않는 특성을 가지는 온 칩 메모리부(201)에 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)를 모두 기록함으로써 기밀 정보의 보안성을 더 높일 수 있다는 이점이 있다.

도8은 본 발명에 따른 기밀 정보 보안 장치의 다른 실시예를 도시한 블록도이다.

도8을 참조하면, 본 발명에 따른 온 칩 메모리 장치를 이용한 기밀 정보 보안 장치(800)는 온 칩 메모리부(801), 메모리 컨트롤러(802), 비교 로직부(803), 외부 입출력 핀(805) 및 억세스 제어부(806)를 포함하여 구성될 수 있다.

상기 구성 요소들은 각각 도2에서 예시한 본 발명에 따른 기밀 정보 보안 장치(200)의 온 칩 메모리부(201), 메모리 컨트롤러(202), 비교 로직부(203), 외부 입출력 핀(205) 및 억세스 제어부(206)에 대응되며, 동일한 기능을 수행한다.

그러나, 도2에서 예시한 기밀 정보 보안 장치(200)와 비교하면, 도8의 기밀 정보 보안 장치(800)는 제 2 보안키 저장부(204)의 구성이 생략된다. 따라서, 제 2 보안키 저장부(204)에 기록되는 제 2 보안키(SEC2KEY) 역시 온 칩 메모리부(801)의 소정 영역(811)에 기록된다는 점에서 차이가 있다.

한편, 제 2 보안키(SEC2KEY)가 온 칩 메모리부(801)의 소정 영역(811)에 기록됨에 따라, 비교 로직부(803)의 내부 구성이 도2의 기밀 정보 보안 장치(200)에 이용되는 비교 로직부(203)의 내부 구성과는 차이가 있다.

도9는 본 발명에 따른 기밀 정보 보안 장치의 다른 실시예에 이용되는 비교 로직부의 한 구성예를 도시한 블록도이다.

도9를 참조하면, 도8의 기밀 정보 보안 장치(800)에 사용될 수 있는 비교 로직부(803)의 한 구성예를 알 수 있다. 도9의 비교 로직부(803)는 제 1 레지스터부(901), 제 2 레지스터부(902), 및 비교부(903)를 포함하여 구성될 수 있다.

도3에서 예시한 비교 로직부(203)의 구성과 비교하여, 도9의 비교 로직부(803)는 온 칩 메모리부(211)에 저장된 두 개의 보안키(SEC1KEY, SEC2KEY)를 각각 읽어들이는 두 개의 레지스터부(901,902)를 포함하여 구성될 수 있다.

제 1 레지스터부(901)는 메모리 컨트롤러(802)를 통하여 상기 온 칩 메모리부(801)의 소정 영역(811)에서 제 1 보안키(SEC1KEY)를 읽어와서 저장하는 역할을 수행한다.

제 2 레지스터부(902)는 메모리 컨트롤러(802)를 통하여 상기 온 칩 메모리부(801)의 소정 영역(811)에서 제 2 보안키(SEC2KEY)를 읽어와서 저장하는 역할을 수행한다.

상기 레지스터부(901,902)의 필요성은 비교부(903)의 구성에 따라서 달라질 수 있다. 도9의 비교 로직부(803)는 제 1 레지스터부(901)와 제 2 레지스터부(902)에 각각 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)의 내용을 모두 옮기고, 비교부(903)에서 비교하는 방식으로 동작한다. 이 경우에, 제 1 레지스터부(901)와 제 2 레지스터부(902)는 상기 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)의 길이만큼의 비트열을 저장할 수 있도록 구성된다.

비교부(903)는 상기한 바와 같이, 레지스터부(901,902)로부터 입력되는 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)를 서로 비교한다. 따라서, 비교부(903)는 적어도 하나의 비교기(comparator; 904)를 포함하여 구성될 수 있고, 상기 레지스터부(901,902)의 구성에 따라서 비교기의 숫자 및 연결이 다양하게 이루어질 수 있다.

도9에서는, 각각 쉬프트 레지스터로 구성된 제 1 레지스터부(901)와 제 2 레지스터부(902)로부터 순차적으로 1비트씩의 정보를 입력받아서 비교기(904)에서 비교 결과를 출력하는 방식으로 동작한다.

비교부(903)는 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)의 비교 결과로서 보안키 비교 신호(COMPARE_RES)를 출력한다. 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)의 모든 비트가 동일하면 보안키 비교 신호(COMPARE_RES)는 '0'을 유지하고, 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)가 한 비트라도 상이하면 보안키 비교 신호(COMPARE_RES)는 '1'로 출력됨은 도3 및 도4의 비교 로직부(203)와 동일하다.

한편, 온 칩 메모리부(801)에 이용될 수 있는 불휘발성 멀티-타임 프로그래머블 셀 어레이의 셀들은 최초 상태에서 공정에 따라서 '0' 또는 '1'의 상태를 유지하고 있게되는 것이 일반적이다. 이에 따라, 온 칩 메모리부(801)로서 사용되는 메모리 셀 어레이에 따라서는, 초기 상태에서 온 칩 메모리부의 소정 영역에서 읽어 들이는 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)는 우연적으로 일치되는 경우가 발생한다. 따라서, 제품 생산 과정 중의 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)를 기록하기 위한 공정에서 외부 입출력 핀(805)을 통한 온 칩 메모리부(801)에 대한 기록 및 변경이 최초부터 불가능해지는 경우를 방지하는 것이 필요하다.

도10은 본 발명에 따른 기밀 정보 보안 장치의 다른 실시예에 이용되는 비교 로직부의 다른 구성예를 도시한 블록도이다.

도10에서 예시하고 있는 비교 로직부는 도9에서 예시한 비교 로직부(803)의 구성 요소들과 동일한 구성 요소들로 구성된다. 다만, 도10의 비교 로직부에는 제 2 레지스터부(902)의 적어도 하나의 비트(905)에 연결되는 퓨즈(fuse; 906)가 추가적으로 포함된다. 초기 상태에서는 퓨즈(906)가 연결된 제 2 레지스터부(902)의 소정 비트(905)는 퓨즈에 의해서 특정값을 유지할 수 있다.

예컨대, 온 칩 메모리부(801)의 셀들의 초기 상태가 '0'이라면, 상기 퓨즈(906)에 연결된 제 2 레지스터부(902)의 소정 비트(905)는 '1'을 유지하도록 구성된다. 반대로, 온 칩 메모리부(801)의 셀들의 초기 상태가 '1'이라면, 상기 퓨즈(906)에 연결된 제 2 레지스터부(902)의 소정 비트(905)는 '0'을 유지하도록 구성된다.

이를 통하여 온 칩 메모리부(801)의 소정 영역(811)에서 읽어들여진 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)가 동일한 경우에도, 제 1 레지스터부(901)와 제 2 레지스터부(902)에 저장되는 값은 차이를 가지도록 구성될 수 있다.

한편, 상기 목적을 위한 퓨즈(906)로는 별도의 퓨즈 커팅(cutting) 공정이 필요한 레이저 커팅 퓨즈가 사용될 수도 있으나, 전기적 퓨즈(electrical fuse)가 이용되는 것이 더욱 바람직하다. 전기적 퓨즈를 사용할 경우에는 제품 생산 과정 중에 외부 입출력 핀(805)을 통하여 온 칩 메모리부(801)에 인증키를 포함한 기밀 정보를 기록한 다음, 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)를 기록하고, 전기적 퓨즈를 프로그래밍하는 과정을 연속성있게 진행할 수 있는 이점이 있다.

도11은 본 발명에 따른 기밀 정보 보안 장치의 다른 실시예에 이용되는 비교 로직부의 레지스터부 동작을 예시한 흐름도이다.

도11을 참조하면, 도9에서 예시한 본 발명의 기밀 정보 보안 장치(800)에 이용될 수 있는 비교 로직부(803)의 레지스터부(901,902)의 동작이 설명된다.

시스템이 파워 온 되거나 리셋되어 메모리 컨트롤러(802)가 리셋 신호(RESET)를 수신하면, 비교 로직부(803)의 레지스터부(901,902)로의 제 1,2 보안키(SEC1KEY, SEC2KEY) 로딩이 시작된다(S111).

먼저, 리셋 신호(RESET)를 수신한 메모리 컨트롤러(802)는 로드 완료 신호(LOAD)를 '로우'로 비활성화시킨다(S112). 로드 완료 신호(LOAD)는 억세스 제어부(806)에 입력되어, 칩 외부로부터의 억세스 요청을 온 칩 메모리부(801)로 전달할 것인지를 결정하는 신호로서 이용된다.

다음으로, 온 칩 메모리부(801)로부터 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)를 읽어들여 레지스터부(901,902)로 옮기는 단계(S113 및 S114)가 진행된다.

레지스터부(901,902)의 구성과 온 칩 메모리부(801)를 구성하는 메모리 셀 어레이의 특성에 따라서 달라질 수 있으나, 도11에서는 8비트 단위로 온 칩 메모리부(801)의 소정 영역(811)에서 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)를 읽어들여 8비트 단위로 구성된 레지스터부(901,902)에 저장하는 과정을 예시하고 있다. 예컨대, 제 1 보안키(SEC1KEY)가 32비트 길이를 가진다면, 4번의 리드 사이클(read cycle)만에 제 1 보안키가 레지스터부(301)에 로드된다.

온 칩 메모리부(801)로부터 레지스터부(901,902)로의 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)의 로딩이 완료되면, 메모리 컨트롤러(802)는 로드 완료 신호(LOAD)를 '하이'로 활성화시켜 억세스 제어부(806)로 전달하면서(S115), 비교 로직부(803)의 보안키 로딩 동작이 완료된다(S116).

도12는 본 발명에 따른 기밀 정보 보안 방법의 다른 실시예의 전체적인 흐름도이다.

도12를 참조하면, 본 발명의 기밀 정보 보안 방법의 전체적인 동작을 알 수 있다. 도12에서 예시한 흐름도는 도8에서 예시한 기밀 정보 보안 장치(800), 특히 도10의 비교 로직부 구성을 채용한 기밀 정보 보안 장치를 기준으로 하여 구성된 것이지만, 도12에서 예시하고 있는 기밀 정보 보안 방법은 본 발명에 따른 기밀 정보 보안 장치의 다른 구성에도 적용될 수 있음은 자명하다.

메인 칩이 파워 온 되거나 리셋되면 본 발명의 기밀 정보 보안 방법이 시작된다(S121).

온 칩 메모리부(801)의 소정 영역(811)에 기록된 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)가 서로 비교된다(S122). 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)의 비교는 기밀 정보 보안 장치(800)의 비교 로직부(803)에서 이루어지는 동작으로, 비교 로직부(803)의 구성에 따라서, 다르게 이루어질 수 있음은 도9 및 도10을 통하여 이미 설명된 바와 같다.

한편, 상기 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)를 비교하는 단계에서 메모리 컨트롤러(802)를 통하여 온 칩 메모리부(801)에 기록된 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)를 읽어들이는 동안에는 칩 외부로부터의 억세스 신호를 원천적으로 차단하는 과정이 추가적으로 요구될 수 있다.

제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)를 온 칩 메모리부(801)로부터 비교 로직부(803)로 로드하기 위한 절차와 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)의 로드 진행 중에 억세스 신호의 원천적인 차단 절차는 상기 도 11에서 예시한 흐름도에 의해 이루어질 수 있음은 이미 설명된 바와 같다.

다음으로, 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)가 동일한지 여부를 판단한다(S123). 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)가 동일한 경우에는 비교 로직부(803)가 출력하는 보안키 비교 신호(COMPARE_RES)는 '0'으로 유지된다(S124_1). 반대로 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)가 상이한 경우에는 비교 로직부(803)가 출력하는 보안키 비교 신호(COMPARE_RES)는 '1'로 유지된다(S124_2).

칩 외부로부터 활성화된 테스트 인에이블 신호(TEST_EN)와 억세스 신호(E_ADDR, E_CTRL, E_DIO)를 수신하면 칩 외부로부터의 억세스 신호의 허용 여부를 판단하는 절차가 진행된다(S125).

테스트 인에이블 신호(TEST_EN)가 활성화된 상태에서 보안키 비교 신호(COMPARE_RES)의 상태를 판단한다(S126).

보안키 비교 신호(COMPARE_RES)가 '0' 상태이면, 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)가 동일한 경우이므로 이미 동일한 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)가 온 칩 메모리부(801)의 소정 영역(811)에 기록된 상태임을 의미한다. 따라서, 칩 외부로부터의 억세스 신호는 차단된다(S127).

반대로, 보안키 비교 신호(COMPARE_RES)가 '1' 상태이면, 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)가 상이한 경우이므로 아직 동일한 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)가 온 칩 메모리부(801)의 소정 영역(811)에 기록되지 않은 상태임을 의미한다. 따라서, 칩 외부로부터의 억세스 신호(E_ADDR, E_CTRL, E_DIO)는 온 칩 메모리부(801)에 전달된다(S128). 따라서, 상기 억세스 신호에 의해서 온 칩 메모리부(801)에는 인증키를 포함한 기밀 정보가 기록 또는 검증될 수 있다.

최종적으로 보안키 비교 신호(COMPARE_RES)가 '1'인 상태에서, 기밀 정보의 기록이 완료되면, 온 칩 메모리부(801)의 소정 영역(811)에 동일한 제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)를 기록한다(S129).

제 1 보안키(SEC1KEY)와 제 2 보안키(SEC2KEY)가 기록된 다음에는 퓨즈 프로그래밍이 실시된다(S130). 퓨즈는 도10에서 설명된 바 있는 온 칩 메모리부(801)의 소정 영역(811)에서 읽어들인 제 1 보안키와 제 2 보안키가 우연적으로 동일하여 초기 기밀 정보 기록을 불가능한 현상을 방지하기 위한 것이다.

마지막으로, 시스템이 파워 다운(power down)되거나, 시스템 리셋 신호가 인가되면 온 칩 메모리부(801)에 대한 외부로부터의 더 이상의 억세스는 차단된다(S131).

상기에서는 본 발명의 바람직한 실시예를 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허 청구의 범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다. 특히, 모듈 형태로 구성된 시스템들은 매우 다양한 서로 다른 성분과 기능들을 조합하여 구성될 수 있다는 것은 너무 잘 알려져 있다. 따라서 실제 구현에 있어서는 본 발명의 각 구성요소들의 일부분들이 혼합될 수도 있고, 각 구성요소들이 그룹지어진 다른 이름의 구성요소로서 존재할 수도 있다.

발명의 효과

상기와 같은 본 발명에 따르면, 기밀 정보가 기록되는 온 칩 메모리 장치의 소정 영역에 제 1 보안키를 저장하고, 제 2 보안키는 별도의 메모리 장치 또는 온 칩 메모리 장치에 같이 저장하여, 양 보안키의 비교 결과를 이용하여 칩 외부로부터의 억세스 요청의 허용 여부를 결정하도록 한다.

따라서, 본 발명의 기밀 정보 보안 장치가 적용된 제품은, 제품의 생산 과정에서는 기밀 정보의 저장 및 변경을 가능하게 하고, 제품이 출하된 다음에는 기밀 정보의 파괴 및 유출을 방지할 수 있도록 하는 효과를 가져올 수 있다.

도면의 간단한 설명

도1은 종래 기술의 온 칩 메모리 장치를 이용한 기밀 정보 보안 장치의 블록도이다.

도2는 본 발명에 따른 기밀 정보 보안 장치의 블록도이다.

도3은 본 발명의 기밀 정보 보안 장치에 이용되는 비교 로직부의 한 구성예를 도시한 블록도이다.

도4는 본 발명의 기밀 정보 보안 장치에 이용되는 비교 로직부의 다른 구성예를 도시한 블록도이다.

도5는 본 발명의 기밀 정보 보안 장치에 이용되는 비교 로직부의 레지스터부 동작을 예시한 흐름도이다.

도6은 본 발명의 기밀 정보 보안 장치에 이용되는 억세스 제어부의 구성예를 도시한 블록도이다.

도7은 본 발명의 기밀 정보 보안 방법의 전체적인 흐름도이다.

도8은 본 발명에 따른 기밀 정보 보안 장치의 다른 실시예를 도시한 블록도이다.

도9는 본 발명에 따른 기밀 정보 보안 장치의 다른 실시예에 이용되는 비교 로직부의 한 구성예를 도시한 블록도이다.

도10은 본 발명에 따른 기밀 정보 보안 장치의 다른 실시예에 이용되는 비교 로직부의 다른 구성예를 도시한 블록도이다.

도11은 본 발명에 따른 기밀 정보 보안 장치의 다른 실시예에 이용되는 비교 로직부의 레지스터부 동작을 예시한 흐름도이다.

도12는 본 발명에 따른 기밀 정보 보안 방법의 다른 실시예의 전체적인 흐름도이다.

* 도면의 주요부분에 대한 부호의 설명 *

200: 기밀 정보 보안 장치

201: 온 칩 메모리부 202: 메모리 컨트롤러

203: 비교 로직부 204: 제 2 보안키 저장부

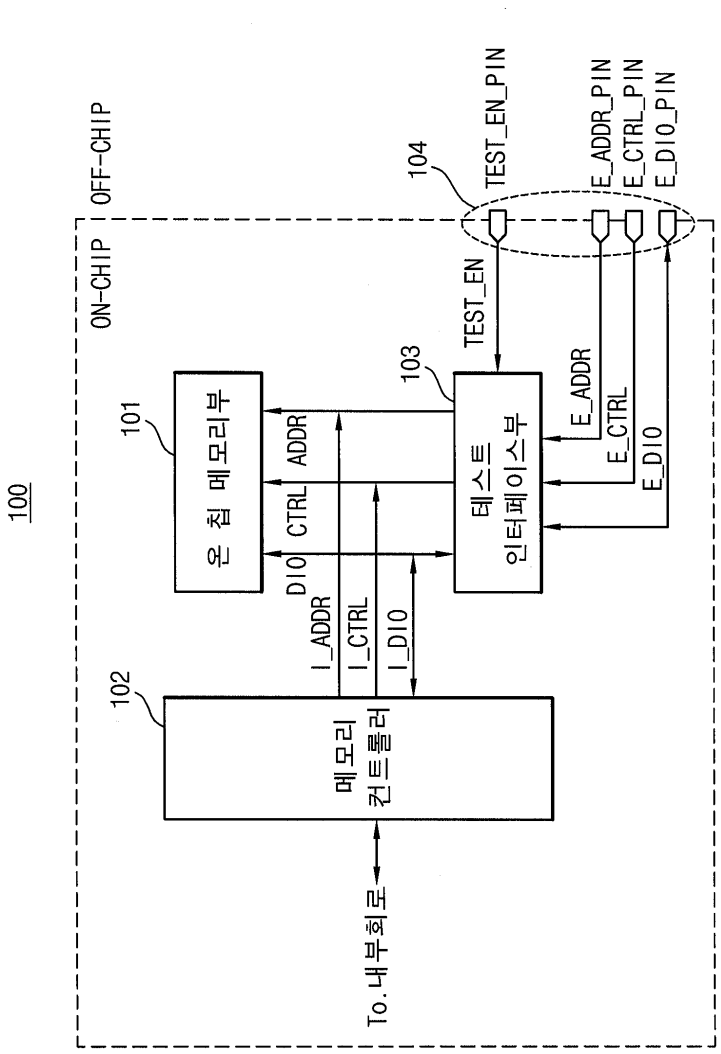
205: 외부 입출력 핀 206: 억세스 제어부

SEC1KEY: 제 1 보안키 SEC2KEY: 제 2 보안키

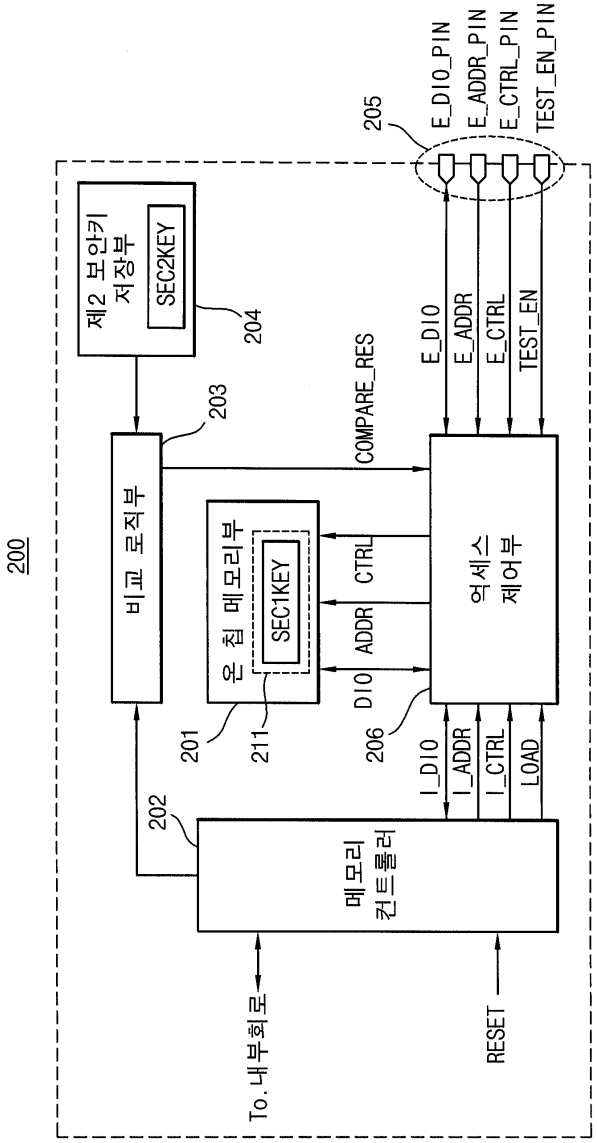
COMPARE_RES: 보안키 비교 신호

도면

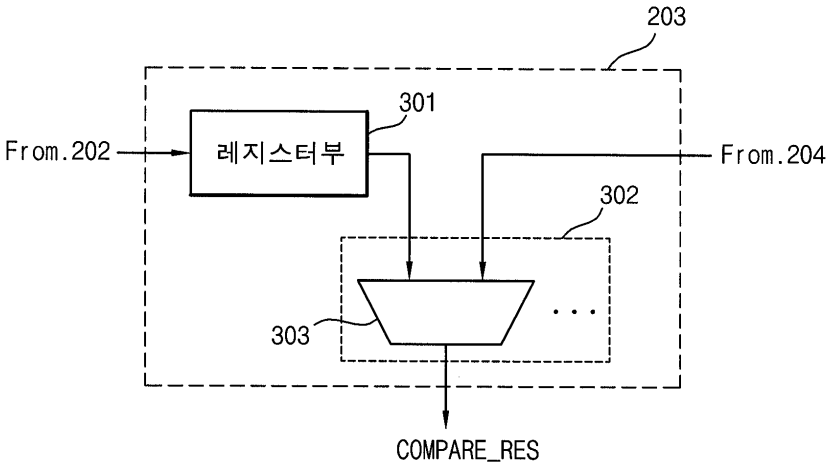
도면1


100
OFF-CHIP
ON-CHIP
104
TEST_EN_PIN
E_ADDR_PIN
E_CTRL_PIN
E_DIO_PIN
TEST_EN
103
101
온 칩 메모리부
ADDR
CTRL
DIO
테스트
인터페이스부
E_ADDR
E_CTRL
E_DIO
I_ADDR
I_CTRL
I_DIO
102
메모리
컨트롤러
To. 내부회로

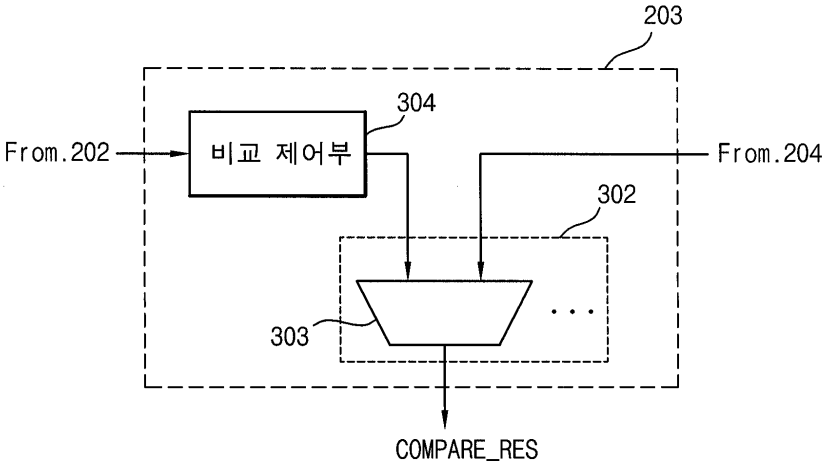
도면2


200
205
E_DIO_PIN
E_ADDR_PIN
E_CTRL_PIN
TEST_EN_PIN
제2 보안키 저장부
SEC2KEY
204
203
비교 로직부
COMPARE_RES
E_DIO
E_ADDR
E_CTRL
TEST_EN
온 칩 메모리부
SEC1KEY
CTRL
ADDR
DIO
억세스 제어부
201
211
206
I_DIO
I_ADDR
I_CTRL
LOAD
202
메모리 컨트롤러
To.내부회로
RESET

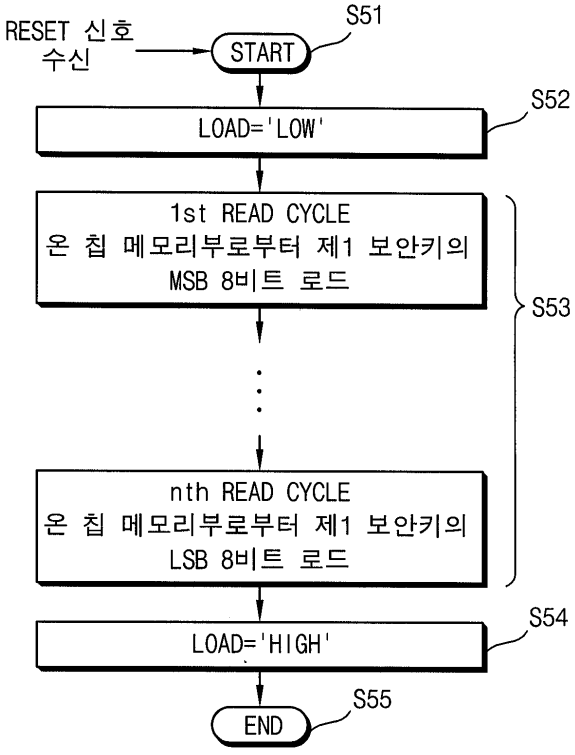
도면3


203
301
From.202
레지스터부
From.204
302
303
COMPARE_RES

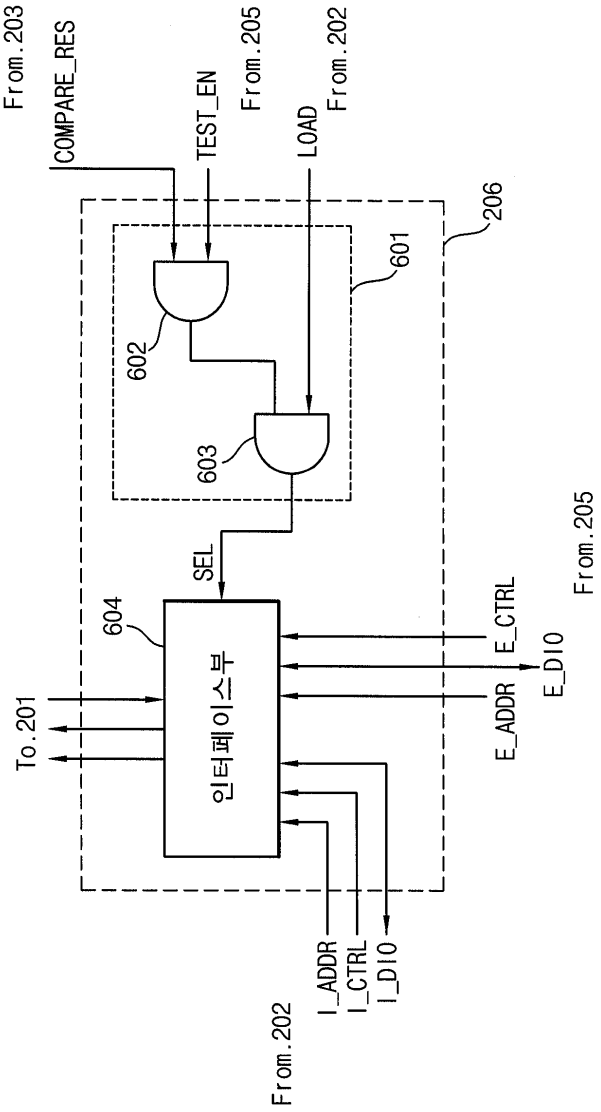
도면4


203
304
From.202
비교 제어부
From.204
302
303
COMPARE_RES

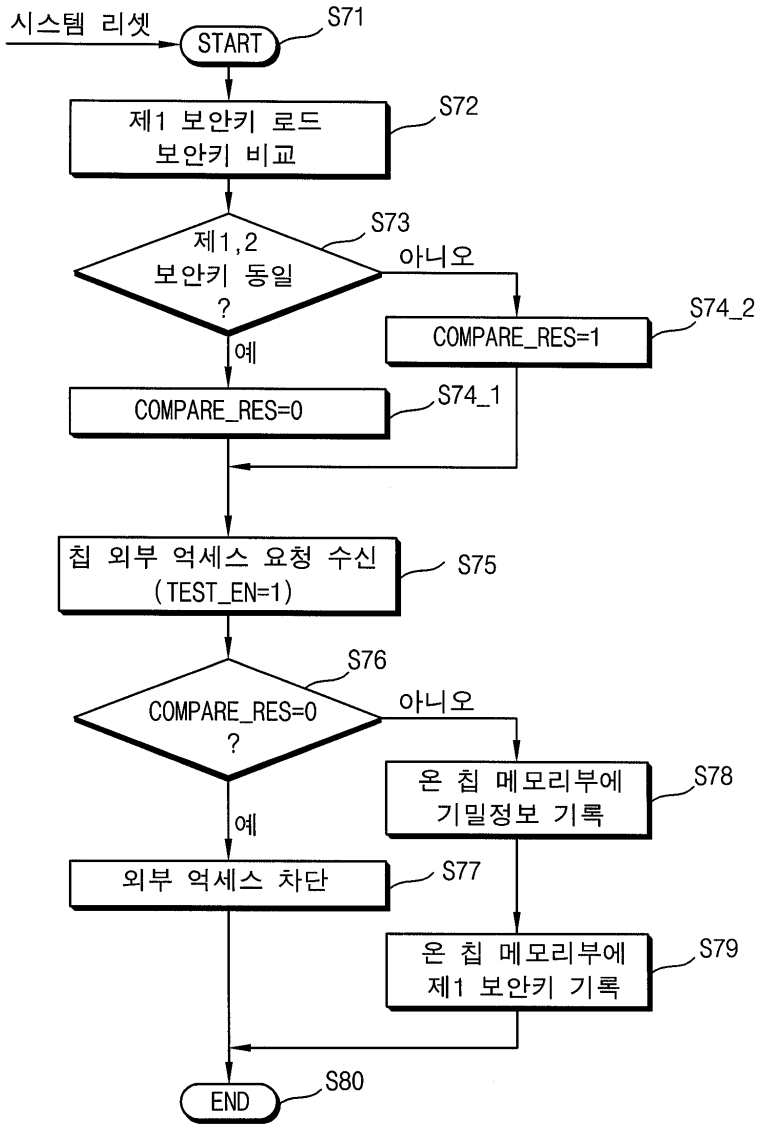
도면5


RESET 신호
수신
START
S51
LOAD='LOW'
S52
1st READ CYCLE
온 칩 메모리부로부터 제1 보안키의
MSB 8비트 로드
S53
nth READ CYCLE
온 칩 메모리부로부터 제1 보안키의
LSB 8비트 로드
LOAD='HIGH'
S54
END
S55

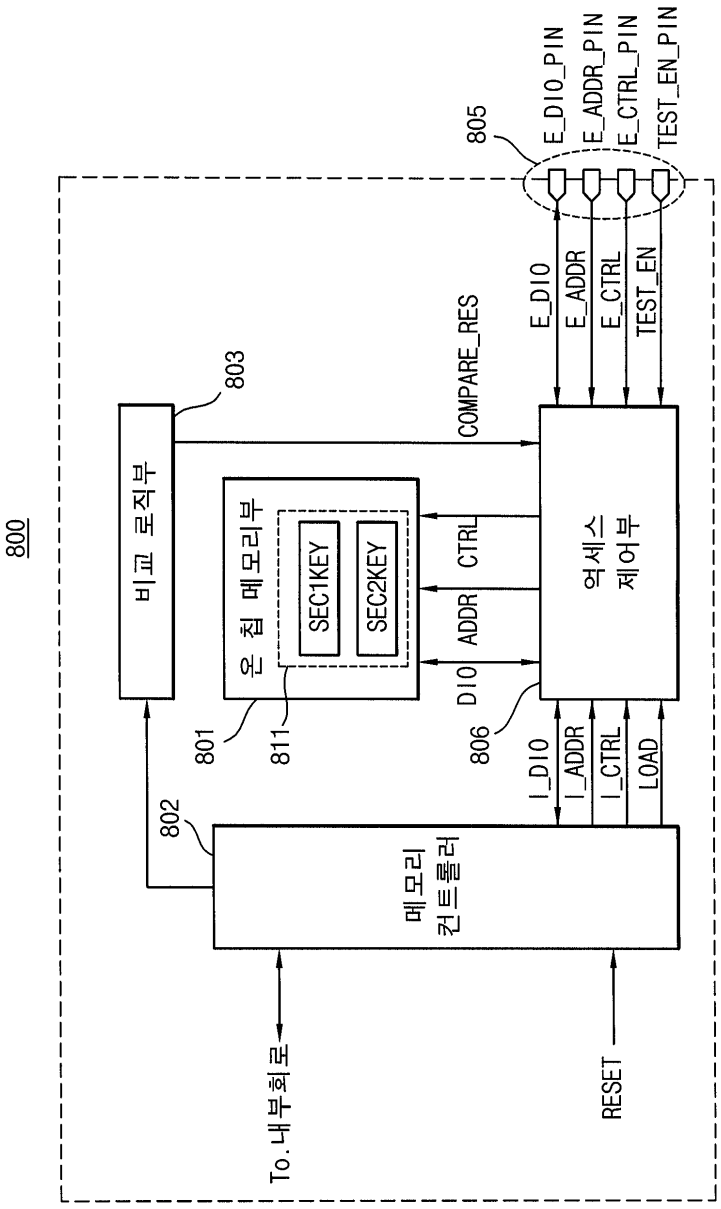
도면6


From.203
COMPARE_RES
TEST_EN
From.205
LOAD
From.202
206
601
602
603
SEL
604
인터페이스부
To.201
E_CTRL
E_DIO
E_ADDR
From.205
I_ADDR
I_CTRL
I_DIO
From.202

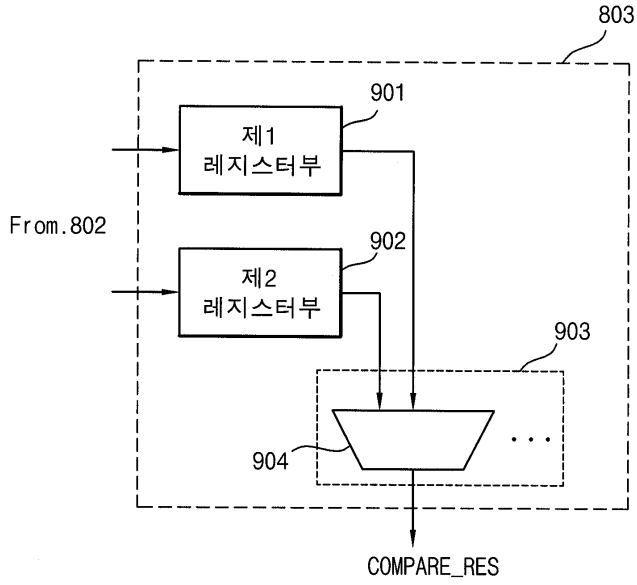
도면7


시스템 리셋
START
S71
제1 보안키 로드
보안키 비교
S72
제1,2
보안키 동일
?
S73
아니오
예
COMPARE_RES=1
S74_2
COMPARE_RES=0
S74_1
칩 외부 억세스 요청 수신
(TEST_EN=1)
S75
COMPARE_RES=0
?
S76
아니오
예
온 칩 메모리부에
기밀정보 기록
S78
외부 억세스 차단
S77
온 칩 메모리부에
제1 보안키 기록
S79
END
S80

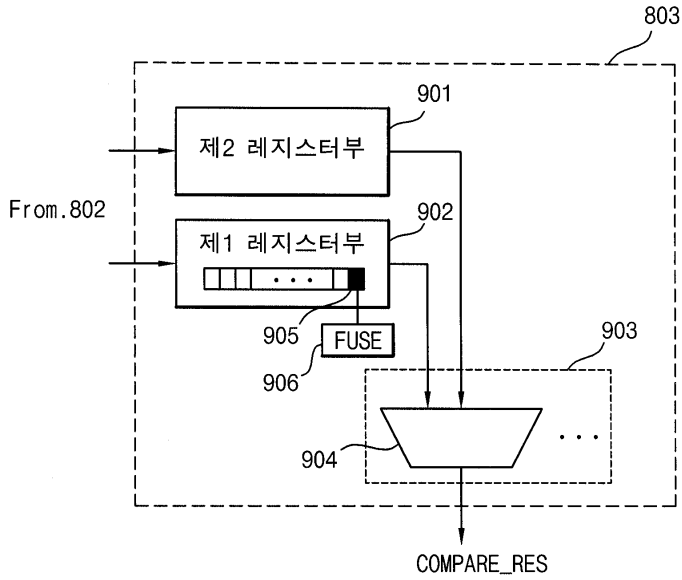
도면8


800
805
E_DIO_PIN
E_ADDR_PIN
E_CTRL_PIN
TEST_EN_PIN
E_DIO
E_ADDR
E_CTRL
TEST_EN
COMPARE_RES
803
비교 로직부
온 칩 메모리부
SEC1KEY
SEC2KEY
CTRL
ADDR
DIO
억세스 제어부
801
811
806
I_DIO
I_ADDR
I_CTRL
LOAD
802
메모리 컨트롤러
To.내부회로
RESET

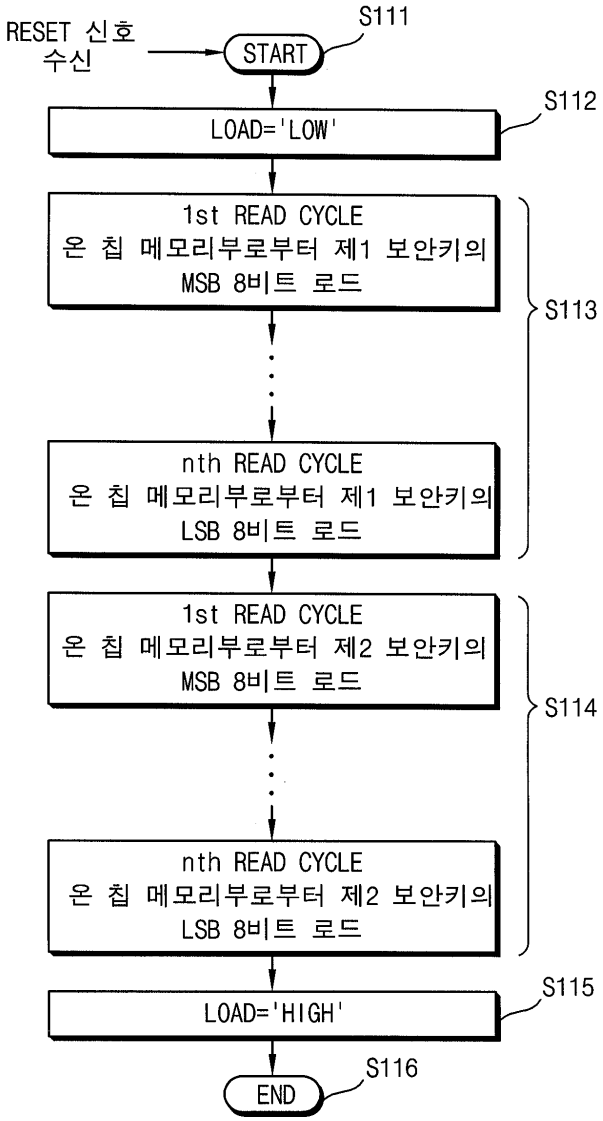
도면9


803
901
제1
레지스터부
From.802
902
제2
레지스터부
903
904
COMPARE_RES

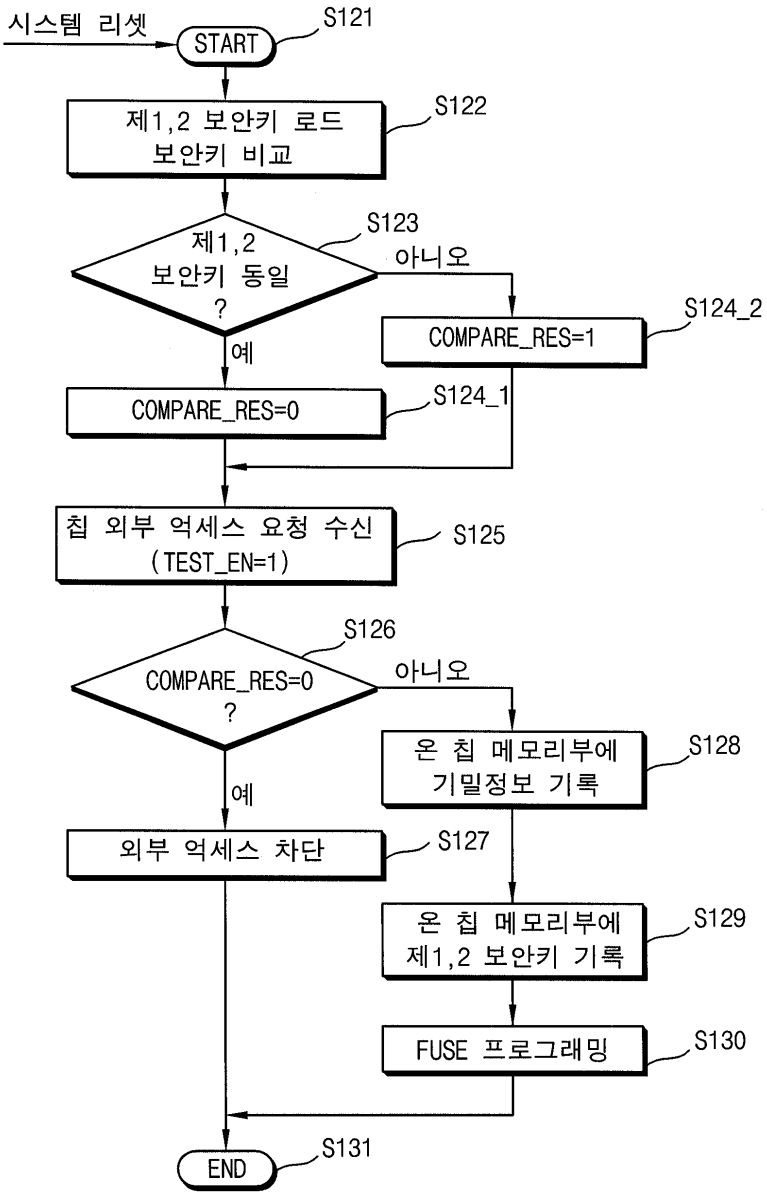
도면10


803
901
제2 레지스터부
From.802
902
제1 레지스터부
905
FUSE
906
903
904
COMPARE_RES

도면11


RESET 신호 수신
START
S111
LOAD='LOW'
S112
1st READ CYCLE
온 칩 메모리부로부터 제1 보안키의 MSB 8비트 로드
nth READ CYCLE
온 칩 메모리부로부터 제1 보안키의 LSB 8비트 로드
S113
1st READ CYCLE
온 칩 메모리부로부터 제2 보안키의 MSB 8비트 로드
nth READ CYCLE
온 칩 메모리부로부터 제2 보안키의 LSB 8비트 로드
S114
LOAD='HIGH'
S115
END
S116

도면12


시스템 리셋
START
S121
제1,2 보안키 로드
보안키 비교
S122
제1,2
보안키 동일
?
S123
아니오
예
COMPARE_RES=1
S124_2
COMPARE_RES=0
S124_1
칩 외부 억세스 요청 수신
(TEST_EN=1)
S125
COMPARE_RES=0
?
S126
아니오
예
온 칩 메모리부에
기밀정보 기록
S128
외부 억세스 차단
S127
온 칩 메모리부에
제1,2 보안키 기록
S129
FUSE 프로그래밍
S130
END
S131