(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2008년04월17일
(11) 등록번호 10-0823374
(24) 등록일자 2008년04월11일

(51) Int. Cl.
*G06F 15/00* (2006.01) *G06F 21/00* (2006.01)
*G06F 1/00* (2006.01)
(21) 출원번호 10-2006-7027677(분할)
(22) 출원일자 2006년12월28일
심사청구일자 2006년12월28일
번역문제출일자 2006년12월28일
(65) 공개번호 10-2007-0014208
(43) 공개일자 2007년01월31일
(62) 원출원 특허 10-2004-7020945
원출원일자 2004년12월23일
심사청구일자 2004년12월23일
(86) 국제출원번호 PCT/US2003/019597
국제출원일자 2003년06월20일
(87) 국제공개번호 WO 2004/003711
국제공개일자 2004년01월08일
(30) 우선권주장
10/185,887 2002년06월26일 미국(US)
(56) 선행기술조사문헌
EP 1085396 A
US 6275933 B1
전체 청구항 수 : 총 12 항

(73) 특허권자
**인텔 코오퍼레이션**
미합중국 캘리포니아 산타클라라 미션 칼리지 블러바드 2200
(72) 발명자
**그래우코크, 데이비드**
미국 97007 오레곤주 알로하 사우스웨스트 184번 애비뉴 8285
**포이스너, 데이비드**
미국 95630 캘리포니아주 폴섬 펜리 스퀘어 205
(74) 대리인
**백만기, 이중희, 주성민**

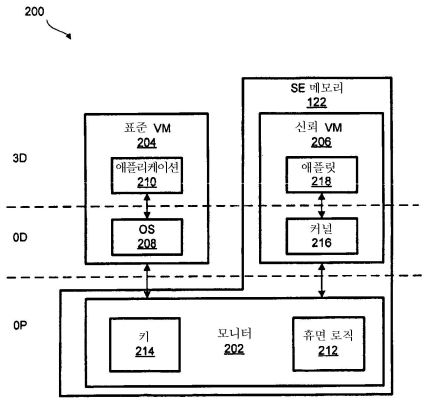
심사관 : 천대녕

## (54) 휴면 보호

*(57) 요 약*

휴면 공격으로부터 비밀을 보호하는 방법, 장치 및 기계 판독 가능 매체가 개시된다. 몇몇 실시예에서, 휴면 상태에 들어가기 전에 비밀은 암호화되고, 보안 강화 환경이 제거된다. 몇몇 실시예는 웨이크 이벤트에 응답하여 보안 강화 환경을 재설정하고, 비밀을 해독한다.

*대표도* - 도2



## *특허청구의 범위*

**청구항 1**

운영 체제 및 보다 우선 순위를 갖는 모니터를 포함하고,

상기 운영 체제는 휴면 이벤트를 수신하고, 상기 모니터에 상기 휴면 이벤트의 처리를 전송하며,

상기 모니터는 휴면 요구에 응답하여 메모리의 하나 이상의 페이지를 암호화하고, 상기 메모리가 암호화되지 않은 비밀 데이터를 보유하지 않음을 표시하는 시스템.

**청구항 2**

제1항에 있어서, 상기 모니터는 상기 메모리가 암호화되지 않은 비밀 데이터를 보유하지 않음을 표시하기 위하여 비밀 저장소를 더 갱신하는 시스템.

**청구항 3**

제1항에 있어서,

상기 모니터는 상기 운영 체제에 상기 휴면 이벤트의 처리를 반환하며,

상기 운영 체제는 메모리의 암호화된 페이지 및 암호화되지 않은 페이지들을 불휘발성 저장소에 기입하는 시스템.

**청구항 4**

제1항에 있어서,

상기 모니터는 상기 운영 체제에 상기 휴면 이벤트의 처리를 반환하고,

상기 운영 체제는 상기 시스템이 휴면 상태에 진입하도록 하는 시스템.

**청구항 5**

제4항에 있어서, 상기 운영 체제는 진입하게 되는 휴면 상태를 표시하도록 휴면 타입 저장소를 갱신하고, 상기 휴면 상태로의 진입을 호출하도록 휴면 인에이블 저장소를 갱신하는 시스템.

**청구항 6**

제1항에 있어서, 상기 모니터는 상기 메모리의 암호화된 페이지들을 증명하는 내용 증명서를 더 생성하는 시스템.

**청구항 7**

제6항에 있어서, 상기 모니터는 상기 암호화된 페이지들을 식별하는 구조를 더 생성하고, 상기 구조를 증명하는 구조 증명서를 생성하는 시스템.

**청구항 8**

제7항에 있어서, 상기 모니터는 상기 모니터에 상기 내용 증명서, 상기 구조 증명서 및 상기 암호화된 페이지들을 해독하기 위한 모니터 키를 더 봉인하는 시스템.

**청구항 9**

보안 강화 영역을 포함하는 휘발성 메모리;

상기 휘발성 메모리가 암호화되지 않은 비밀 데이터를 보유할 수 있는지를 지시하는 비밀 저장소;

휴면 상태로의 진입을 호출하는 휴면 인에이블 저장소;

휴면 이벤트에 응답하여 상기 보안 강화 영역을 암호화하고, 상기 보안 강화 영역의 암호화에 응답하여 상기 휘발성 메모리가 암호화되지 않은 비밀 데이터를 보유하지 않음을 지시하도록 상기 비밀 저장소를 갱신하는 프로

세서; 및

상기 휴면 인에이블 저장소가 휴면 상태로의 진입을 호출하도록 갱신되고, 상기 비밀 저장소가 상기 휘발성 메모리가 암호화되지 않은 비밀 데이터를 보유할 수 있음을 지시하는 것에 응답하여, 휴면 공격 응답을 호출하는 휴면 공격 검출 로직

을 포함하는 시스템.

**청구항 10**

제9항에 있어서, 상기 프로세서는 상기 보안 강화 영역을 증명하는 내용 증명서를 더 생성하고, 상기 내용 증명서가 상기 보안 강화 영역이 신빙성이 없음을 지시하는 경우 웨이크 이벤트에 응답하여 휴면 공격 응답을 호출하는 시스템.

**청구항 11**

제10항에 있어서, 상기 프로세서는 상기 시스템에 상기 내용 증명서 및 상기 보안 강화 영역을 해독하기 위한 키를 더 봉인하는 시스템.

**청구항 12**

제11항에 있어서, 상기 프로세서는 상기 내용 증명서 및 상기 키의 봉인 해제가 실패하는 경우 웨이크 이벤트에 응답하여 휴면 공격 응답을 더 호출하는 시스템.

# *명 세 서*

## *발명의 상세한 설명*

### *발명의 목적*

#### *발명이 속하는 기술 및 그 분야의 종래기술*

<11> 금융 및 개인 거래가 컴퓨팅 장치 상에서 수행되는 비율이 증가하고 있다. 그러나, 이러한 금융 및 개인 거래의 계속적인 성장은 프라이버시의 훼손, 데이터의 변조, 데이터의 남용 등을 방지하기 위한 보안 강화(security enhanced; SE) 환경의 설정에 부분적으로 의존한다. SE 환경은 보호된 데이터 또는 비밀(예를 들어, 사회 보장 번호, 계좌 번호, 은행 잔고, 패스워드, 인증 키 등)에 대한 여러 종류의 공격 또는 비인증 액세스를 방지하기 위한 다양한 기술을 이용할 수 있다. SE 환경이 방지할 수 있는 일 유형의 공격은 휴면 공격(sleep attack)이다.

#### *발명이 이루고자 하는 기술적 과제*

<12> 예를 들어, 많은 컴퓨팅 장치들은 예를 들어 Advanced Configuration and Power Interface (ACPI) Specification, revision 2.0, 27 July 2000에 기술된 S3 휴면 상태와 같은 서스펜드-투-메모리(suspend-to-memory) 휴면 상태를 지원한다. 서스펜드-투-메모리 휴면 상태에 들어갈 때, 컴퓨팅 장치는 컴퓨팅 장치의 각종 컴포넌트들 및/또는 서브 컴포넌트들로부터 전력을 제거하지만, 시스템 메모리의 내용을 유지하기 위하여 시스템 메모리에는 계속 전력을 공급한다. 전력 제거의 결과, 컴퓨팅 장치는 시스템 메모리에 저장된 비밀을 보호하는 데 사용되는 회로로부터 전력을 제거할 수 있다. 휴면 상태로부터 깨어날 때, 컴퓨팅 장치는 시스템 메모리에 저장된 비밀을 보호하는 데 사용되는 회로에 전력을 재공급한다. 그러나, 전력의 재공급 후, 보호 회로는 재설정 상태에 있을 수 있어, 실제로 시스템 메모리 내의 비밀을 보호할 수 없게 된다. 보호 회로에 의해 제공되는 보호를 재설정하기 전에 공격자가 저장된 비밀에 대한 액세스에 성공할 수 있다.

<13> 본 발명은 이러한 휴면 공격으로부터 비밀을 보호하기 위한 기술을 제공한다.

### *발명의 구성 및 작용*

<14> 본 명세서에 기재된 발명은 첨부 도면들에서 제한하는 것이 아니라 예시적으로 도시되어 있다. 도시의 간결성 및 명확성을 위해, 도면들에 도시된 요소들은 반드시 축척에 따라 그려진 것은 아니다. 예를 들어, 몇몇 요소들의 치수는 명확성을 위해 다른 요소들에 비해 확대될 수 있다. 또한, 적당하다고 생각되는 경우, 도면 부호

들은 대응하거나 유사한 요소들을 표시하기 위해 도면들 사이에서 반복되어 있다.

<15> <실시예>

<16> 이하의 설명은 휴면 공격으로부터 비밀을 보호하기 위한 기술들을 설명한다. 이하의 설명에서는 본 발명의 더욱 철저한 이해를 제공하기 위하여, 논리 구현, 연산 코드(opcode), 피연산자(operand) 지정 수단, 자원 분할/공유/복제 구현, 시스템 컴포넌트들의 타입 및 상호관계, 및 논리 분할/통합 선택과 같은 많은 특정 세부 사항들이 설명된다. 그러나, 당업자들은 본 발명이 그러한 특정 세부 사항 없이도 실시될 수 있다는 것을 이해할 것이다. 다른 예에서는, 발명을 모호하게 하지 않기 위하여 제어 구조, 게이트 레벨 회로 및 전체의 소프트웨어 명령 시퀀스들이 상세히 도시되지 않았다. 당업자들은 포함된 설명으로부터 과도한 실험 없이도 적당한 기능을 구현할 수 있을 것이다.

<17> 명세서에서 "일 실시예", "실시예" 등에 대한 참조는 기재된 실시예가 특정 특징, 구조 또는 특성을 포함할 수 있지만, 모든 실시예가 특정 특징, 구조 또는 특성을 반드시 포함할 수 있는 것이 아니라는 것을 나타낸다. 더욱이, 이러한 문구는 반드시 동일 실시예를 참조하고 있지는 않다. 또한, 실시예와 관련하여 특정 특징, 구조 또는 특성이 설명될 때, 명백히 설명되어 있는지의 여부와 관계 없이 다른 실시예들과 관련하여 상기 특징, 구조 또는 특성을 달성하는 것은 당업자의 지식 내에 있는 것이라 할 수 있다.

<18> 본 명세서에서 "대칭" 암호 작성, 키, 암호화 또는 해독에 대한 참조는 동일 키가 암호화 및 해독을 위해 사용되는 암호 기술을 지칭한다. 연방 정보 출판 표준(FIPS) PUB 46-2로서 1993년에 발표된 공지의 데이터 암호화 표준(DES) 및 FIPS PUB 197로서 2001년에 발표된 고급 암호화 표준(AES)은 대칭 암호법의 예들이다. 본 명세서에서 "비대칭" 암호 작성, 키, 암호화 또는 해독에 대한 참조는 상이하지만 관련이 있는 키들이 암호화 및 해독에 각각 사용되는 암호 기술을 지칭한다. 공지의 Rivest-Shamir-Adleman(RSA) 기술을 포함하는 소위 "공용 키" 암호 기술들은 비대칭 암호법의 예들이다. 비대칭 암호 시스템의 2개의 관련 키들 중 하나는 본 명세서에서 비밀 키(일반적으로 비밀로 유지되므로)로서 지칭되고, 다른 키는 공용 키(일반적으로 자유롭게 이용할 수 있으므로)로서 지칭된다. 몇몇 실시예에서 비밀 키 또는 공용 키는 암호화를 위해 사용될 수 있고, 다른 키는 관련된 해독을 위해 사용될 수 있다.

<19> 본 명세서에서 사용하는 "객체"라는 용어는 구조, 포맷 또는 표현에 관계없이 하나 이상의 비트의 임의의 그룹화를 포함하는 포괄적인 용어인 것으로 의도된다. 또한, "해시"라는 동사 및 관련 형태들은 본 명세서에서 다이제스트 값 또는 "해시"를 생성하기 위하여 피연산자 또는 메시지에 연산을 수행하는 것을 지칭하는 데 사용된다. 이상적으로, 해시 연산은 그 해시로 메시지를 찾는 것이 계산적으로 불가능하고 그 해시로 메시지에 대한 임의의 사용 가능한 정보를 결정할 수 없는 다이제스트 값을 생성한다. 또한, 해시 연산은 동일 해시를 생성하는 2개의 메시지를 결정하는 것이 계산적으로 불가능하도록 해시를 이상적으로 생성한다. 해시 연산이 이상적으로 상기 특성을 갖지만, 실제로는 예를 들어 메시지 다이제스트 5 기능(MD5) 및 보안 해싱 알고리즘 1(SHA-1)과 같은 단방향 기능들은 메시지를 추론해내는 것이 어렵고, 계산적으로 집약적이며, 및/또는 실제로 불가능한 해시 값들을 생성한다.

<20> 본 발명의 실시예들은 하드웨어, 펌웨어, 소프트웨어 또는 이들의 임의의 조합으로 구현될 수 있다. 또한, 본 발명의 실시예들은 하나 이상의 프로세서에 의해 판독되어 실행될 수 있는 기계 판독 가능 매체 상에 저장된 명령들로서 구현될 수 있다. 기계 판독 가능 매체는 기계(예를 들어 컴퓨팅 장치)에 의해 판독될 수 있는 형태로 정보를 저장 및 전송하는 임의의 메커니즘을 포함할 수 있다. 예를 들어, 기계 판독 가능 매체는 ROM, RAM, 자기 디스크 저장 매체, 광학 저장 매체, 플래시 메모리 장치, 전기, 광학, 음향 또는 기타 형태의 전파 신호(예를 들어, 반송파, 적외선 신호, 디지탈 신호 등) 등을 포함할 수 있다.

<21> 컴퓨팅 장치(100)의 예시적인 실시예가 도 1에 도시되어 있다. 컴퓨팅 장치(100)는 프로세서 버스(106)를 통해 칩셋(104)에 결합된 하나 이상의 프로세서들(102)을 포함할 수 있다. 칩셋(104)은 프로세서(102)를 시스템 메모리(108), 토큰(110), 펌웨어(112), 불휘발성 저장 장치(114)(예를 들어, 하드 디스크, 플로피 디스크, 광 디스크, 플래시, 프로그래머블 판독 전용 메모리 등) 및/또는 기타 장치들(116)(예를 들어, 마우스, 키보드, 비디오 제어기 등)에 결합시키는 하나 이상의 집적 회로 패키지 또는 칩을 포함할 수 있다.

<22> 프로세서들(102)은 예를 들어 도 2의 예시적인 SE 환경과 같은 SE 환경의 생성을 개시하기 위한 보안 진입(SENTER) 명령의 실행을 지원할 수 있다. 프로세서들(102)은 또한 SE 환경의 해제를 개시하기 위한 보안 해제(SEXIT) 명령을 지원할 수 있다. 일 실시예에서, 프로세서(102)는 SENTER, SEXIT 및 다른 명령들의 실행과 관련하여 프로세서 버스(106) 상에서 버스 메시지를 발행할 수 있다.

<23> 프로세서들(102)은 또한 예를 들어 대칭 암호 키, 비대칭 암호 키 또는 몇몇 다른 타입의 키와 같은 키(118)를 포함할 수 있다. 프로세서(102)는 인증 코드(AC) 모듈을 실행하기 전에 프로세서 키(118)를 사용하여 AC 모듈을 인증할 수 있다. 일 실시예에서, 프로세서 키(118)는 프로세서(102)만이 액세스할 수 있는 비대칭 비밀 키를 포함한다.

<24> 프로세서들(102)은 예를 들어 리얼 모드, 보호 모드, 가상 리얼 모드 및 가상 기계 모드(VMX 모드)와 같은 하나 이상의 동작 모드를 지원할 수 있다. 또한, 프로세서들(102)은 지원된 동작 모드 각각에서 하나 이상의 우선 순위 또는 링(ring)을 지원할 수 있다. 일반적으로, 프로세서(102)의 동작 모드 및 우선 순위는 실행에 이용할 수 있는 명령들 및 이들 명령을 실행한 결과를 정의한다. 구체적으로, 프로세서(102)는 적당한 모드 및/또는 우선 순위에 있을 때에만 소정의 우선 명령들을 실행할 수 있다.

<25> 칩셋(104)은 프로세서들(102)을 예를 들어 시스템 메모리(108), 토큰(110), 불휘발성 기억 장치(114) 및 기타 장치들(116)과 같은 컴퓨팅 장치(100)의 컴포넌트들과 인터페이스하게 하는 하나 이상의 칩셋 또는 집적 회로 패키지를 포함할 수 있다. 일 실시예에서, 칩셋(104)은 메모리 제어기(120)를 포함한다. 그러나, 다른 실시예에서 프로세서(102)는 메모리 제어기(120)의 모두 또는 일부를 포함할 수 있다. 일반적으로, 메모리 제어기(120)는 시스템 메모리(108)에 액세스할 수 있도록 컴퓨팅 장치(100)의 컴포넌트들에게 인터페이스를 제공한다. 또한, 칩셋(104) 및/또는 프로세서들(102)의 메모리 제어기(120)는 메모리(108)의 소정의 영역을 보안 강화(SE) 메모리(122)로서 정의할 수 있다. 일 실시예에서, 프로세서들(102)은 단지 적당한 동작 모드(예를 들어 보호 모드) 및 우선 순위(예를 들어 OP)에 있을 때 SE 메모리(122)에 액세스할 수 있다.

<26> 또한, 칩셋(104)은 실행 전에 AC 모듈을 인증하는 데 사용될 수 있는 키(124)를 포함할 수 있다. 프로세서 키(118)와 유사하게, 칩셋 키(124)는 대칭 암호 키, 비대칭 암호 키 또는 소정의 다른 타입의 키를 포함할 수 있다. 일 실시예에서, 칩셋 키(124)는 칩셋(104)만이 액세스할 수 있는 비대칭 비밀 키를 포함한다. 다른 실시예에서, 칩셋(104)은 컴퓨팅 장치(100)의 다른 컴포넌트에 저장된 비대칭 칩셋 키(124)의 해시를 포함한다. 칩셋(104)은 칩셋 키(124)를 검색하고, 해시를 사용하여 키(124)를 인증할 수 있다.

<27> 칩셋(104)은 시스템 메모리(108)가 암호화되지 않은 비밀들을 포함할 수 있는지를 지시하는 비밀 저장소(126)를 더 포함할 수도 있다. 일 실시예에서, 비밀 저장소(126)는 시스템 메모리(108)가 암호화되지 않은 비밀들을 포함할 수 있음을 지시하도록 설정될 수 있고, 시스템 메모리(108)가 암호화되지 않은 비밀들을 포함하지 않음을 지시하도록 소거될 수 있는 플래그를 포함할 수 있다. 다른 실시예에서, 비밀 저장소(126)는 예를 들어, 토큰(110), 프로세서들(102) 또는 컴퓨팅 장치(100)의 다른 컴포넌트들과 같이 어딘가 다른 곳에 배치될 수 있다.

<28> 일 실시예에서, 비밀 저장소(126)는 배터리에 의해 제공되는 백업 전력을 갖는 단일 불휘발성 메모리 비트로서 구현된다. 배터리에 의해 공급되는 백업 전력은 시스템 재설정, 휴면 이벤트, 시스템 셧다운, 시스템 파워 다운 또는 기타 전력 제거/손실 이벤트 시에 비밀 저장소(126)의 내용을 유지한다. 칩셋(104)은 또한 배터리에 의해 제공되는 전력의 인터럽션을 검출하기 위한 배터리 검출 회로(도시되지 않음)를 포함할 수 있다. 이 회로는 또한 시스템 메모리(108)가 전력 인터럽션의 검출에 응답하여 비밀들을 유지할 수 있음을 지시하도록 비밀 저장소(126)를 갱신할 수 있다. 다른 실시예에서, 비밀 저장소(126)는 전력 제거/손실 이벤트 시에 그 내용을 유지하기 위하여 백업 전력을 필요로 하지 않는 플래시 메모리 비트와 같은 불휘발성 메모리 비트로서 구현된다. 일 실시예에서, 비밀 저장소(126)는 설정 또는 소거될 수 있는 단일 메모리 비트로 구현된다. 그러나, 다른 실시예는 다른 저장 용량을 갖고, 및/또는 다른 상태 인코딩을 이용하는 비밀 저장소(126)를 포함할 수 있다.

<29> 칩셋(104)은 또한 비인증 갱신들로부터 비밀 저장소(126)를 더 보호할 수 있다. 일 실시예에서, 칩셋(104)은 프로세서 버스(106)의 처리를 디코딩하고, 및/또는 프로세서(102)로부터 메시지를 수신하기 위한 프로세서 인터페이스(128)를 포함한다. 프로세서들(102)은 칩셋(104)에게 비밀 저장소(126)를 갱신할 것을 요구하는 하나 이상의 우선 명령을 실행하는 것에 응답하여 버스 처리 및/또는 메시지를 생성할 수 있다. 프로세서 인터페이스(128)는 버스 처리 및/또는 메시지를 수신하고, 디코딩된 버스 처리 및/또는 메시지에 기초하여 비밀 저장소(126)를 갱신할 수 있다. 일 실시예에서, 우선 명령의 유효 실행은 특정 프로세서 우선 순위로 실행되는 소프트웨어로 제한된다. 예를 들어, 일 실시예에서 우선 명령의 유효 실행은 최우선 프로세서 순위로 실행되는 모니터로 제한된다(도 2 참조).

<30> 칩셋(104)은 또한 비밀 저장소(126)의 비우선 갱신을 허용할 수 있다. 일 실시예에서, 프로세서들(102)은 하나 이상의 우선 명령의 실행에 응답하여 칩셋(104)에게 비밀 저장소(126)의 비우선 갱신을 허용하도록 요구하는 버

스 처리 및/또는 메시지를 생성할 수 있다. 또한, 프로세서들(102)은 하나 이상의 비우선 또는 우선 명령의 실행에 응답하여 칩셋(104)에게 비밀 저장소(126)의 비우선 갱신을 거부하도록 요구하는 버스 처리 및/또는 메시지를 생성할 수 있다. 프로세서들(102)은 하나 이상의 비우선 명령의 실행에 응답하여 칩셋(104)에게 비밀 저장소(126)를 갱신하도록 요구하는 버스 처리 및/또는 메시지를 생성할 수 있다. 프로세서 인터페이스(128)는 버스 처리 및/또는 메시지를 수신하고, 디코딩된 버스 처리 및/또는 메시지에 기초하여 비우선 갱신을 하용하고, 비우선 갱신을 거부하고, 및/또는 비밀 저장소(126)를 갱신할 수 있다. 일 실시예에서, 비우선 갱신을 요구하기 위한 우선 명령들의 유효 실행은 특정 프로세서 우선 순위로 실행되는 소프트웨어로 제한된다. 예를 들어, 일 실시예에서 이들 우선 명령의 유효 실행은 최우선 프로세서 레벨로 실행되는 모니터로 제한되며, 따라서 모니터가 비밀 저장소(126)에 대한 선택된 비우선 코드(예를 들어 AC 모듈) 기입 액세스를 제공하는 것을 허용한다.

<31> 칩셋(104)은 또한 휴면 제어기(130), 휴면 타입 저장소(132) 및 휴면 인에이블 저장소(134)를 포함할 수 있다. 일 실시예에서 휴면 제어기는 휴면 타입 저장소(132) 및 휴면 인에이블 저장소(134)에 기초하여 컴포넌트들 및/또는 서브 컴포넌트들에 전력을 선택적으로 전력을 공급한다. 일 실시예에서, 휴면 제어기(130)가 컴퓨팅 장치(100)를 배치하는 휴면 상태(예를 들어 ACPI 휴면 상태들 S1, S2, S3, S4)를 지시하는 값이 휴면 타입 저장소(132)에 저장될 수 있다. 휴면 인에이블 저장소(134)는 휴면 상태 저장소(132)에 의해 지시된 휴면 상태로의 진입을 호출하도록 갱신될 수 있다. 예를 들어, 휴면 인에이블 저장소(134)는 설정에 응답하여 휴면 제어기(130)가 컴퓨팅 장치(100)를 요구된 휴면 상태로 배치하도록 하는 플래그를 포함할 수 있다.

<32> 칩셋(104)은 또한 가능한 휴면 공격을 검출하는 휴면 공격 검출 로직(136)을 포함할 수 있다. 일 실시예에서, 휴면 방법은 시스템 메모리(108)가 휴면 진입 프로세스를 개시하기 위하여 휴면 인에이블 저장소(134)를 갱신하기 전에 암호화되지 않은 비밀들을 포함하지 않음을 지시하도록 비밀 저장소(126)를 갱신한다. 따라서, 일 실시예에서 휴면 공격 검출 로직(136)은 (i) 비밀 저장소(126)가 시스템 메모리(108)가 암호화되지 않은 비밀들을 포함할 수 있음을 지시하는 것, 및 (ii) 휴면 인에이블 저장소(134)가 휴면 진입 프로세스가 호출되는 것을 요구하는 것에 응답하여 휴면 공격이 가능한 것으로 결정한다. 가능한 휴면 공격의 검출에 응답하여, 휴면 공격 검출 로직(136)은 예를 들어 시스템 재설정 이벤트, 시스템 중지 이벤트, 시스템 셧다운 이벤트, 시스템 파워 오프 이벤트, 또는 시스템 메모리(108)에 저장된 비밀을 보호하기 위한 소정의 다른 응답의 생성과 같은 휴면 공격 응답을 개시한다.

<33> 다른 실시예에서, 휴면 공격 검출 로직(136)은 또한 들어가는 휴면 상태에 기초하여 휴면 공격 응답을 호출할 것인지의 여부를 결정한다. 예를 들어, SE 메모리(122)에 저장된 비밀들을 보호하는 데 사용되는 회로는 주어진 휴면 상태 동안 유효할 수 있다. 따라서, 휴면 공격 검출 로직(136)은 휴면 공격이 발생하고 있지 않은 것으로 결정하거나 휴면 타입 저장소(132)가 SE 메모리 보호가 유효한 휴면 상태를 지시하는 경우 휴면 공격 응답을 호출하지 않도록 결정할 수 있다.

<34> 칩셋(104)은 또한 주변 컴포넌트 상호 접속(PCI), 가속 그래픽 포트(AGP), 유니버셜 시리얼 버스(USB), 로우 핀 카운트(LPC) 버스 또는 임의의 다른 종류의 I/O 버스(도시되지 않음)와 같은 I/O 버스들 상에서 표준 I/O 동작을 지원할 수 있다. 구체적으로, 칩셋(104)은 칩셋(104)을 하나 이상의 플랫폼 구성 레지스터(PCR; 140)를 포함하는 토큰(110)과 접속하는 토큰 인터페이스(138)를 포함할 수 있다. 일 실시예에서, 토큰 인터페이스(138)는 LPC 버스 인터페이스(LPC 인터페이스 사양, 인텔사 rev. 1.0, 29 December 1997)를 포함할 수 있다.

<35> 일반적으로, 토큰(110)은 보안 강화 방식으로 메트릭을 기록하고, 보안 강화 방식으로 메트릭을 인용하고, 비밀들을 특정 환경(현재 또는 미래)에 봉인하고, 비밀들을 봉인 해제하여 이들이 봉인 제공된 환경에 제공할 수 있다. 토큰(110)은 상기 동작들을 지원하는 데 사용될 수 있는 하나 이상의 키(142)를 포함할 수 있다. 토큰 키(142)는 대칭 키, 비대칭 키 및/또는 소정의 다른 타입의 키를 포함할 수 있다. 토큰(110)은 또한 보안 강화 방식으로 메트릭을 기록하고 보고하는 하나 이상의 플랫폼 구성 레지스터(PCR 레지스터; 140)를 포함할 수 있다. 일 실시예에서, 토큰(110)은 수신된 메트릭을 식별된 PCR 레지스터(140)에 보안 강화 방식으로 기록하는 PCR 확장 동작을 지원한다.

<36> 토큰(110)은 또한 식별된 PCR 레지스터(140)의 인용구 또는 내용을 반환하는 PCR 인용 동작을 지원할 수 있다. 토큰(110)은 또한 봉인 동작 및 봉인 해제 동작을 지원할 수 있다. 봉인 동작에 응답하여, 토큰(110)은 토큰 및 특정 장치 환경에 봉인된 객체를 포함하는 봉인된 객체를 생성한다. 역으로, 토큰(110)은 객체가 토큰(110)의 키로 봉인되었고, 현재의 장치 환경이 봉인된 객체에 대해 특정된 환경 기준을 만족시키는 경우에만 봉인 해제 동작에 응답하여 봉인된 객체의 객체를 반환할 수 있다. 일 실시예에서, 토큰(110)은 Trusted Computing

Platform Alliance (TCPA) Main Specification, Version 1.1a, 1 December 2001 또는 그 변형에 기술된 신뢰가능한 플랫폼 모듈(TPM)을 포함할 수 있다.

<37> 일 실시예에서, 펌웨어(112)는 기본 입출력 시스템 루틴(BIOS; 144)을 포함한다. BIOS(144)는 AC 모듈, 휴면 코드, 웨이크 코드, 시스템 시동 코드 및/또는 구조체를 포함할 수 있다. 예를 들어, BIOS(144)는 휴면 이벤트 처리, 웨이크 이벤트 처리 및/또는 컴퓨팅 장치 초기화 동안 액세스 및/또는 실행될 수 있는 ACPI 구조체 및 ACPI 소스 언어(ASL) 코드를 포함할 수 있다.

<38> SE 환경(200)의 일 실시예가 도 2에 도시되어 있다. SE 환경(200)은 예를 들어 시스템 시동, 애플리케이션 요구, 운영 체제 요구 등과 같은 각종 이벤트에 응답하여 개시될 수 있다. 도시된 바와 같이, SE 환경(200)은 신뢰 가상 기계 커널 또는 모니터(202), 하나 이상의 표준 가상 기계(표준 VM; 204) 및 하나 이상의 신뢰 가상 기계(신뢰 VM; 206)를 포함할 수 있다. 일 실시예에서, SE 환경(200)의 모니터(202)는 보안을 관리하고 가상 기계들(204, 206) 사이의 장벽을 제공하기 위하여 최우선 프로세서 링(예를 들어 0P)에서 보호 모드로 실행된다.

<39> 표준 VM(204)은 VMX 모드의 최우선 프로세서 링(예를 들어 0D)에서 실행되는 운영 체제(208), 및 VMX 모드의 저우선 프로세서 링(예를 들어 3D)에서 실행되는 하나 이상의 애플리케이션(210)을 포함할 수 있다. 모니터(202)가 실행되는 프로세서 링이 운영 체제가 실행되는 프로세서 링보다 더 우선적이기 때문에, 운영 체제(208)는 컴퓨팅 장치의 자유로운 제어를 갖지 못하는 대신 모니터(202)의 제어 및 제한을 받는다. 구체적으로, 모니터(202)는 운영 체제(208) 및 그 애플리케이션(210)이 SE 메모리(122) 및 토큰(110)에 직접 액세스하는 것을 방지할 수 있다.

<40> 모니터(202)는 또한 휴면 로직(212) 및 정보를 암호화 및/또는 보호하는 하나 이상의 모니터 키(214)를 포함할 수 있다. 휴면 로직(212)은 예를 들어 메모리 내용의 암호화 및 증명과 같은 하나 이상의 휴면 동작을 수행하기 위한 코드를 포함한다. 모니터 키(214)는 대칭 암호화 키, 비대칭 암호화 키 또는 모니터(202)가 독점적인 제어를 갖는 기타 키를 포함할 수 있다. 예를 들어, 모니터 키(214)는 대칭 루트 키 및 이 대칭 루트 키로 암호화되는 하나 이상의 비대칭 키를 포함할 수 있다.

<41> 모니터(202)는 하나 이상의 메트릭을 얻기 위한 커널 코드의 해시와 같은 신뢰 커널(216)의 하나 이상의 측정을 수행하고, 토큰(110)이 커널(216)의 메트릭으로 PCR 레지스터(140)를 확장하게 하고, SE 메모리(122)에 저장된 관련 PCR 로그에 메트릭을 기록할 수 있다. 모니터(202)는 또한 SE 메모리(122)에 신뢰 VM(206)을 설정하고, 설정된 신뢰 VM(206)에 신뢰 커널(216)을 론칭할 수 있다.

<42> 유사하게, 신뢰 커널(216)은 하나 이상의 메트릭을 얻기 위한 애플릿 코드의 해시와 같은 애플릿 또는 애플리케이션(218)의 하나 이상의 측정을 행할 수 있다. 그러면, 신뢰 커널(216)은 모니터(202)를 통해 물리적 토큰(110)이 애플릿(218)의 메트릭으로 PCR 레지스터(140)를 확장하게 할 수 있다. 신뢰 커널(216)은 또한 SE 메모리(122)에 저장된 관련 PCR 로그에 메트릭을 기록할 수 있다. 또한, 신뢰 커널(216)은 SE 메모리(122)의 설정된 신뢰 VM(206)에 신뢰 애플릿(218)을 론칭할 수 있다.

<43> 도 2의 SE 환경(200)의 개시에 응답하여, 컴퓨팅 장치(100)는 또한 토큰(110)의 하나 이상의 PCR 레지스터(140)에 컴퓨팅 장치(100)의 모니터(202) 및 하드웨어 컴포넌트들의 메트릭을 기록한다. 예를 들어, 프로세서(102)는 예를 들어 프로세서 패밀리, 프로세서 버젼, 프로세서 마이크로코드 버젼, 칩셋 버젼 및 프로세서(102), 칩셋(104) 및 물리적 토큰(110)의 물리적 토큰 버젼과 같은 하드웨어 식별자를 얻을 수 있다. 그러면, 프로세서(102)는 얻은 식별자를 하나 이상의 PCR 레지스터(140)에 기록할 수 있다.

<44> 도 3을 참조하면, 휴면 상태에 들어가기 위한 방법의 일 실시예가 도시된다. 컴퓨팅 장치(100)는 휴면 이벤트에 응답하여 상기 방법을 수행할 수 있다. 예를 들어, 휴면 이벤트는 장치가 소정 기간 동안 유휴 상태로 유지되고 있음을 장치 및/또는 운영 체제가 검출한 것에 응답하여 생성될 수 있다. 휴면 이벤트에 응답하여, 운영 체제(208)는 블록 300에서 SE 환경(200)이 현재 설정되어 있는지의 여부를 판단할 수 있다. SE 환경(200)이 설정되어 있지 않다는 판단에 응답하여, 컴퓨팅 장치(100)는 블록 302에서 컴퓨팅 장치(100)를 요구된 휴면 상태로 배치하기 위한 휴면 진입 프로세스(후술됨)를 호출할 수 있다.

<45> SE 환경(200)이 설정되어 있다는 판단에 응답하여, 모니터(202)는 블록 304에서 SE 메모리(122)의 내용을 암호화 및 증명할 수 있다. 일 실시예에서, 모니터(202)는 모니터 키(214) 중 하나를 이용하여 SE 메모리(122)의 페이지들을 암호화하고, 페이지들을 암호화된 페이지들로 대체한다. 모니터(202)는 모니터(202)를 포함하는 SE 메모리(122)의 일부 또는 모니터(202)의 휴면 로직(212)을 포함하는 SE 메모리(122)의 일부를 암호화되지 않게

남겨 두어 프로세서(102)가 계속 휴면 로직(212)을 실행하게 할 수 있다.

<46> 모니터(202)는 또한 블록 304에서 SE 메모리(122)의 내용을 증명할 수 있다. 일 실시예에서, 모니터(202)는 메모리 해시를 얻기 위해 SE 메모리(122)의 암호화된 내용을 해시함으로써 내용 증명을 생성할 수 있다. 다른 실시예에서, 모니터(202)는 웨이크 프로세스 후 SE 메모리(122) 내에 남을 페이지들만을 해시함으로써 내용 증명을 생성할 수 있다. 예를 들어, 웨이크 프로세스는 불휘발성 저장 장치(114)로부터 모니터(202) 및/또는 다른 코드를 다시 로딩할 수 있다. 이러한 SE 메모리(122)의 부분들은 다시 로딩되므로, 컴퓨팅 장치(100)는 시스템 메모리(108)로부터 이들 부분을 소거할 수 있고, 및/또는 휴면 상태로 들어가기 전에 이들을 불휘발성 저장 장치(114)에 저장하지 않을 수 있다. 또 다른 실시예에서, 모니터(202)는 예를 들어 워터마크, 사인 및/또는 기타 정보와 같은 내용 증명을 SE 메모리(122)의 증명된 내용에 삽입함으로써 SE 메모리(122)의 내용을 증명할 수 있다.

<47> 블록 306에서, 모니터(202)는 블록 304에서 암호화된 시스템 메모리(122)의 페이지/세그먼트/영역을 식별하는 데이터 구조(예를 들어 페이지 테이블, 페이지 리스트, 세그먼트 리스트, 영역 리스트 등)를 생성하고 증명할 수 있다. 일 실시예에서, 모니터(202)는 데이터 구조 해시를 얻기 위해 데이터 구조를 해시함으로써 데이터 구조 증명을 생성할 수 있다. 다른 실시예에서, 모니터(202)는 예를 들어 워터마크, 사인 및/또는 기타 정보와 같은 데이터 구조 증명을 증명된 데이터 구조에 삽입함으로써 데이터 구조를 증명할 수 있다.

<48> 블록 308에서 모니터(202)는 내용 증명서, 데이터 구조 증명서 및/또는 모니터 키(214)를 봉인하여 이들을 비인증 액세스 및/또는 변경으로부터 보호할 수 있다. 일 실시예에서 모니터(202)는 내용 증명서, 데이터 구조 증명서 및 모니터 키(214)를 토큰(110)의 하나 이상의 봉인 동작을 통해 봉인하여 하나 이상의 봉인된 복귀 객체를 얻을 수 있다. 일 실시예에서, 봉인 동작은 모니터(202)의 메트릭을 포함하는 PCR 레지스터(140)를 사용하여 예를 들어 결함 모니터와 같은 다른 모니터가 봉인된 복귀 객체의 암호화되지 않은 내용을 액세스 및/또는 변경하는 것을 효과적으로 방지한다.

<49> 블록 310에서, 모니터(202)는 SE 환경(200)을 제거한다. 모니터(202)는 제거 프로세서의 일부로서 다양한 동작을 행할 수 있다. 일 실시예에서, 모니터(202)는 시스템 메모리(108)가 암호화되지 않은 비밀들을 포함하지 않음을 지시하도록 비밀 저장소(126)를 갱신한다. 예를 들어, 모니터(202)는 시스템 메모리(108)가 암호화되지 않은 비밀들을 포함하지 않음을 지시하도록 비밀 저장소(126)의 플래그를 소거할 수 있다. 또한, 모니터(202)는 신뢰 가상 기계(206)를 셧다운시키고 VMX 프로세서 모드에서 나올 수 있다. 또한, 모니터(202)는 웨이크 프로세스 동안 불휘발성 저장 장치(114)로부터 다시 로딩되는 시스템 메모리(108)의 영역들을 소거할 수 있다.

<50> 블록 312에서, 컴퓨팅 장치(100)는 모니터(202)의 실행을 중지하고 운영 체제(208)의 실행으로 복귀할 수 있다. 일 실시예에서, 운영 체제(208)로의 복귀의 결과, 모니터(202)는 운영 체제(208)에게 웨이킹에 응답하여 실행될 모니터(202)의 위치 및 크기와 봉인된 복귀 객체의 위치 및 크기를 식별하는 SE 환경 복귀 정보를 제공한다. 그러나, 컴퓨팅 장치(100)는 운영 체제(208)가 웨이크 프로세스 동안 모니터(202) 및 봉인된 복귀 객체를 검색할 수 있게 해주는 다른 메커니즘을 사용할 수 있다. 예를 들어, 모니터(202) 및/또는 봉인된 복귀 객체는 소정의 위치에 또는 BIOS(144)에 의해 설정된 위치에 저장될 수 있다.

<51> 블록 314에서, 운영 체제(208)는 웨이크 프로세스의 일부로서 검색될 수 있도록 복귀 정보를 저장할 수 있다. 운영 체제(208)는 시스템 메모리(108)의 소정의 위치, BIOS(144)에 의해 설정된 위치, 칩셋(104)의 불휘발성 레지스터, 및/또는 기타 위치에 SE 환경 복귀 정보를 저장할 수 있다. 일 실시예에서는, 블록 312에서 모니터(202)가 정보를 적당한 위치에 저장하여, 운영 체제가(208)가 블록 314에서 정보를 저장할 필요가 없게 해준다.

<52> 운영 체제(208) 및/또는 BIOS(144)는 블록 302에서 휴면 진입 프로세스를 완료할 수 있다. 예를 들어, 운영 체제(208) 및/또는 BIOS(144)는 컴퓨팅 장치(100)가 어떤 휴면 상태에 들어가고 있는지를 지시하기 위하여 휴면 타입 저장소(132)에 휴면 타입 식별자를 기입할 수 있으며, 휴면 상태로의 진입을 호출하도록 휴면 인에이블 저장소(134)를 갱신할 수 있다. 일 실시예에서, 운영 체제(208) 및/또는 BIOS(144)는 컴퓨팅 장치(100)가 요구된 휴면 상태와 다른 휴면 상태에 들어가게 할 수 있다. 운영 체제(208) 및/또는 BIOS(144)는 예를 들어 컴퓨팅 장치(100)의 하나 이상의 컴포넌트가 요구된 휴면 상태를 지원하지 않는 것과 같은 다양한 이유로 휴면 상태를 변경하도록 선택할 수 있다. 휴면 타입 저장소(132) 및 휴면 인에이블 저장소(134)의 갱신에 응답하여, 휴면 제어기(130)는 컴퓨팅 장치(100)가 휴면 상태에 들어가게 하고, 휴면 프로세스를 완료할 수 있다. 예를 들어, 휴면 제어기(130)는 컴퓨팅 장치(100)의 컴포넌트들 및/또는 서브 컴포넌트들로부터 전력을 제거하고, 컴포넌트들 및/또는 서브 컴포넌트들이 저전력 동작 모드에 들어가도록 요구하고, 및/또는 시스템 메모리(108)의 내용이 불휘발성 저장 장치(114)에 기입되게 할 수 있다.

<53> 이제 도 4를 참조하여, 휴면 상태로부터의 웨이킹 방법이 설명된다. 컴퓨팅 장치(100)는 웨이크 이벤트에 응답하여 웨이크 방법을 수행할 수 있다. 웨이크 이벤트는 예를 들어 모뎀이 링 이벤트를 검출하는 것, 네트워크 제어기가 네트워크 액티비티를 검출하는 것, 키보드 제어기가 키 프레스를 검출하는 것 등과 같은 다양한 자극에 응답하여 발생할 수 있다. 웨이크 이벤트에 응답하여, 휴면 제어기(130)는 블록 400에서 예를 들어 프로세서(102)를 웨이킹하여 저장된 상태 정보를 불휘발성 저장 장치(114)에서 시스템 메모리(108)로 전송하는 것과 같은 하나 이상의 웨이크 동작을 수행할 수 있다. 일 실시예에서 휴면 제어기(130)는 BIOS(144)의 ASL 및/또는 다른 코드를 실행하는 것에 응답하여 하나 이상의 웨이크 동작을 수행할 수 있다. 웨이크 동작을 수행한 후, 휴면 제어기(130)는 제어를 운영 체제(208)에 전달할 수 있다. 일 실시예에서, 휴면 로직(212)은 웨이크 벡터에 의해 식별되는 위치로부터 운영체제(208)의 실행을 호출한다.

<54> 운영 체제(208)는 블록 402에서 컴퓨팅 장치(100)의 네트워크 제어기, 모뎀, 및/또는 기타 장치들을 웨이킹하는 것과 같은 하나 이상의 웨이크 동작을 수행할 수 있다. 블록 404에서, 운영 체제(208)는 저장된 복귀 정보 및/또는 저장된 복귀 정보의 부재에 기초하여 SE 환경(200)을 복원할 것인지의 여부를 결정한다. SE 환경(200)의 복원 결정에 응답하여, 운영체제(208)는 다양한 동작을 수행한다. 예를 들어, 운영 체제(208)는 컴퓨팅 장치(100)를 구성하고, 및/또는 컴퓨팅 장치(100)의 구성을 검증하는 AC 모듈을 로딩하고, 인증하며, 그의 실행을 개시할 수 있다. 또한, 운영체제(208)는 블록 406에서 복귀 정보에 의해 식별되는 모니터(202)를 로딩하고 그 실행을 호출할 수 있다.

<55> 블록 408에서, 모니터(202)는 토큰(110)의 하나 이상의 봉인 해제 동작을 통해 봉인된 복귀 객체를 봉인 해제하여 내용 증명서, 데이터 구조 증명서 및 모니터 키를 얻을 수 있다. 봉인 해제 동작 실패의 검출(블록 410)에 응답하여, 모니터(202)는 블록 412에서 가능한 휴면 공격을 어드레스하기 위한 휴면 공격 응답을 호출한다. 일 실시예에서, 모니터(202)는 시스템 재설정을 호출하도록 칩셋(104)의 재설정 레지스터에 기입함으로써 휴면 공격 응답을 호출한다. 그러나, 모니터(202)는 예를 들어 프로세서(102)를 중지시키고, 시스템 메모리(108)를 소거하고, 시스템 셧다운을 호출하고, 컴퓨팅 장치(100)로부터 전력을 제거하고, 및/또는 비인증 액세스 및/또는 변경으로부터 비밀을 보호하는 등의 다른 방법으로 응답할 수 있다.

<56> 블록 414에서, 모니터(202)는 데이터 구조 증명서에 기초하여 데이터 구조의 신빙성을 검증한다. 일 실시예에서, 모니터(202)는 계산된 데이터 구조 증명서를 얻기 위해 데이터 구조를 해시한다. 모니터(202)는 또한 계산된 데이터 구조 증명서를 봉인된 복귀 객체로부터 얻은 데이터 구조 증명서와 비교하고, 계산된 증명서가 봉인 해제된 증명서에 대해 소정의 관계(예를 들어 동일함)를 갖는 것에 응답하여 데이터 구조가 신빙성 있는 것이라고 결정한다. 데이터 구조가 신빙성이 없거나 변경되었을 수 있다는 결정에 응답하여, 모니터(202)는 블록 412에서 가능한 휴면 공격을 어드레스하기 위한 휴면 공격 응답을 호출한다.

<57> 모니터(202)는 블록 416에서 시스템 메모리(108)의 일부를 해독하여 해독된 부분을 SE 메모리(122)에 저장할 수 있다. 모니터(202)는 하나 이상의 봉인 해제된 모니터 키(214)를 이용하여 데이터 구조에 의해 식별되는 시스템 메모리(108)의 일부를 해독할 수 있다. 블록 418에서, 모니터(202)는 암호화되거나 해독된 SE 메모리 내용의 신빙성을 검증할 수 있다. 일 실시예에서, 모니터(202)는 계산된 내용 증명서를 얻기 위해 SE 메모리(122)에 추가된 해독된 내용을 해시할 수 있다. 다른 실시예에서, 모니터(202)는 계산된 내용 증명서를 얻기 위해 SE 메모리(122)에 추가되는 암호화된 내용을 해시할 수 있다. 모니터(202)는 또한 계산된 내용 증명서를 봉인 해제된 내용 증명서와 비교하고, 계산된 증명서가 봉인 해제된 증명서와 소정의 관계(예를 들어 동일함)를 갖는 것에 응답하여 내용이 신빙성(예를 들어 변경되지 않음)이 있는 것으로 결정할 수 있다. 내용이 신빙성이 없다(예를 들어 변경됨)는 결정에 응답하여, 모니터(202)는 블록 412에서 가능한 휴면 공격에 대한 공격 응답을 호출할 수 있다. 역으로, 내용이 신빙성이 있다는 결정에 응답하여, 모니터(202)는 운영체제(208)의 실행을 호출함으로서 웨이크 프로세스를 완료한다.

<58> 전술한 휴면 및 웨이크 방법의 실시예는 공격으로부터 비밀을 보호하는 것을 돕는다. 그러나, 공격자는 컴퓨팅 장치(100)가 암호화되지 않은 비밀들이 보호되지 않는 시스템 메모리(108) 및/또는 불휘발성 저장 장치(114) 내에 상주하는 휴면 상태에 있도록 하기 위하여 도 3의 휴면 방법을 회피하려고 시도할 수 있다. 이러한 회피를 방지하기 위하여, 휴면 공격 검출 로직(136)은 가능한 휴면 공격의 검출에 응답하여 시스템 재설정 이벤트 또는 다른 공격 응답을 호출할 수 있다. 도 3의 휴면 방법의 일 실시예에서, 모니터(202)는 휴면 진입 프로세스를 개시하기 위하여 휴면 인에이블 저장소(134)를 갱신하기 전에 시스템 메모리(108)가 암호화되지 않은 비밀들을 포함하고 있지 않다는 것을 지시하도록 비밀 저장소(126)를 갱신한다. 따라서, 휴면 공격 검출 로직(136)은 비밀 저장소(420)가 시스템 메모리(108)가 암호화되지 않은 비밀들을 포함할 수 있다는 것을 지시하는 경우 휴면

인에이블 저장소(134)가 갱신되는 것에 응답하여 휴면 공격 응답을 호출할 수 있다.

<59> 도 3의 휴면 방법의 다른 실시예에서, 모니터(202)는 SE 메모리(122)를 암호화하고, 요구된 휴면 상태가 SE 메모리(122)를 보호하지 못하는 결과를 낳은 경우에만 시스템 메모리(108)가 암호화되지 않은 비밀을 포함하지 않음을 지시하도록 비밀 저장소(126)를 갱신한다. 따라서, 휴면 공격 검출 로직(136)은 비밀 저장소(420)가 시스템 메모리(108)가 암호화되지 않은 비밀들을 포함할 수 있는 것으로 지시하고 휴면 타입 저장소(132)가 SE 메모리(122)가 보호되지 않을 수 있는 휴면 상태를 지시하는 경우 휴면 인에이블 저장소(134)가 갱신되는 것에 응답하여 휴면 공격 응답을 호출할 수 있다.

<60> 본 발명의 소정의 특징들이 실시예를 참조하여 설명되었지만, 이러한 설명은 제한적인 의미로 해석되지 않아야 한다. 본 발명이 속하는 분야의 전문가들에게 자명한 본 발명의 다른 실시예는 물론 상기 실시예들의 다양한 변형은 본 발명의 사상 및 범주 내에 있는 것으로 간주된다.

## *발명의 효과*

<61> 본 발명에 의하면 휴면 공격으로부터 비밀을 보호할 수 있다.

## *도면의 간단한 설명*

<1> 도 1은 컴퓨팅 장치의 일 실시예를 도시하는 도면.

<2> 도 2는 도 1의 컴퓨팅 장치에 의해 설정될 수 있는 보안 강화(SE) 환경의 일 실시예를 도시하는 도면.

<3> 도 3은 도 1의 컴퓨팅 장치의 휴면 방법의 일 실시예를 도시하는 도면.

<4> 도 4는 도 1의 컴퓨팅 장치의 웨이크 방법(wake method)의 일 실시예를 도시하는 도면.

<5> <도면의 주요 부분에 대한 설명>

<6> 104: 칩셋

<7> 130: 휴면 제어기

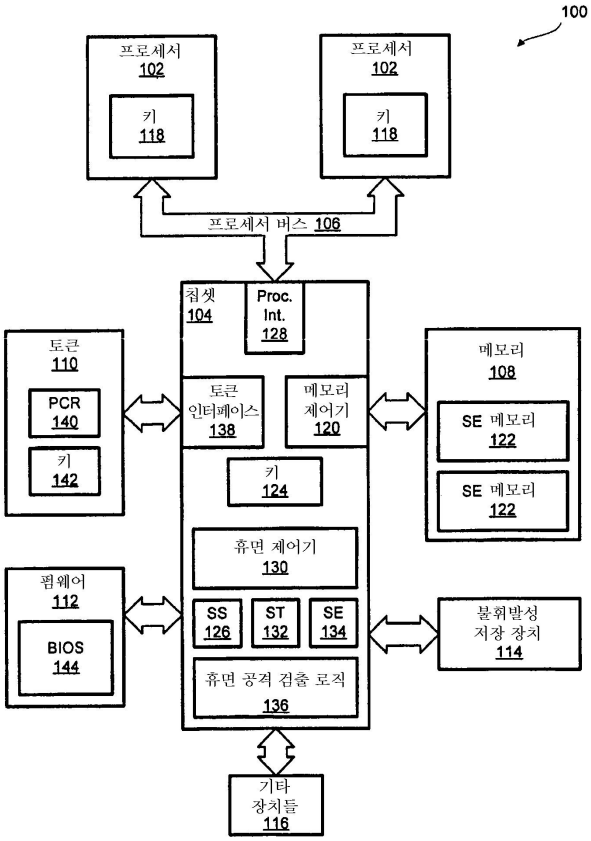
<8> 136: 휴면 공격 검출 로직

<9> 202: 모니터

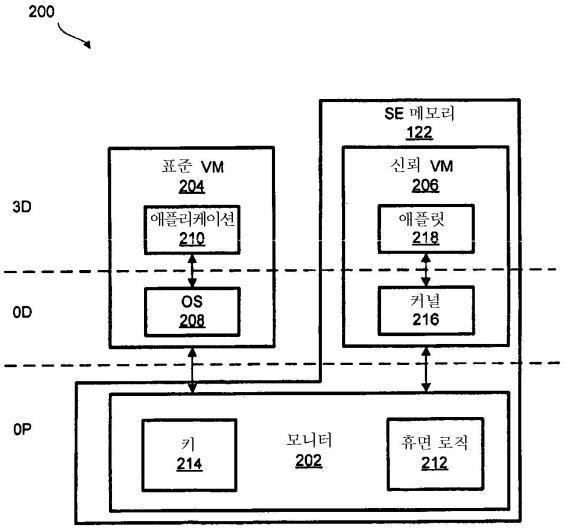
<10> 212: 휴면 로직

## 도면

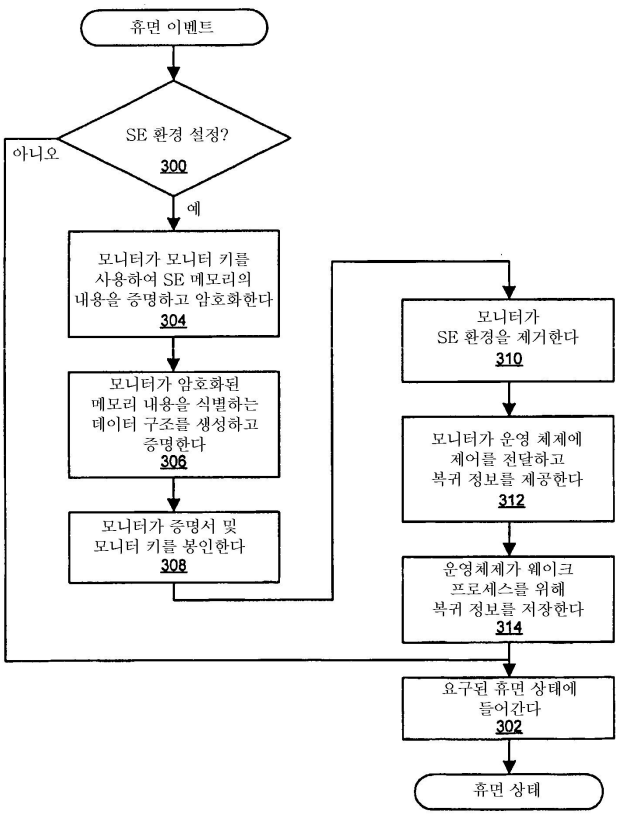
### 도면1


100
프로세서
102
키
118
프로세서
102
키
118
프로세서 버스 106
칩셋
104
Proc.
Int.
128
토큰
110
PCR
140
키
142
토큰
인터페이스
138
메모리
제어기
120
키
124
메모리
108
SE 메모리
122
SE 메모리
122
휴면 제어기
130
펌웨어
112
BIOS
144
SS
126
ST
132
SE
134
휘발성
저장 장치
114
휴면 공격 검출 로직
136
기타
장치들
116

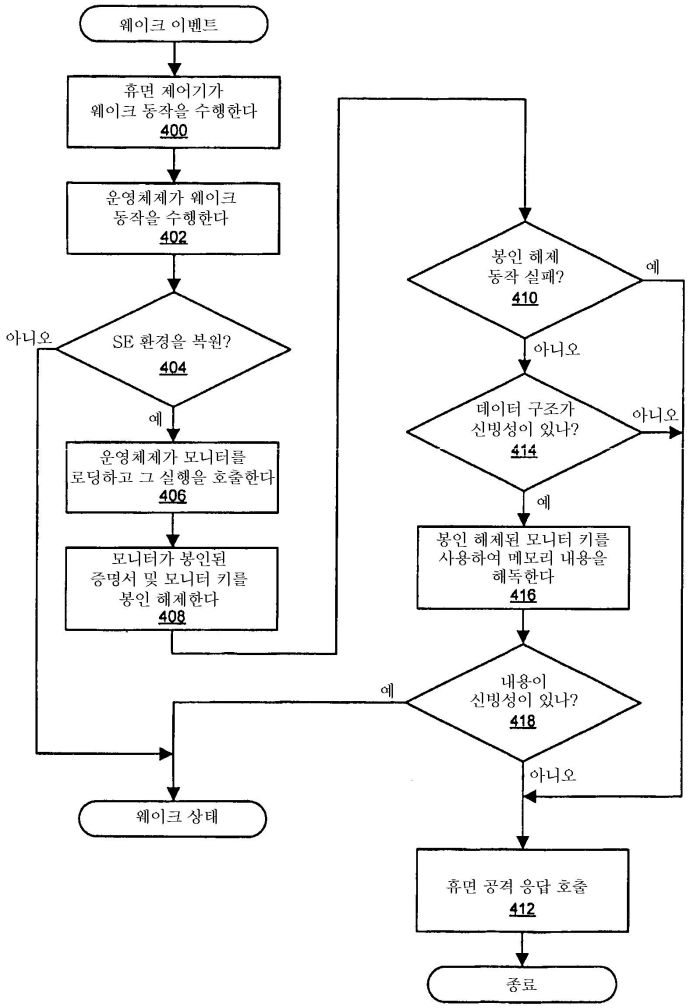
### 도면2


200
SE 메모리
122
표준 VM
204
신뢰 VM
206
3D
애플리케이션
210
애플릿
218
0D
OS
208
커널
216
0P
키
214
모니터
202
휴면 로직
212

도면3


휴면 이벤트
SE 환경 설정?
300
아니오
예
모니터가 모니터 키를 사용하여 SE 메모리의 내용을 증명하고 암호화한다
304
모니터가 암호화된 메모리 내용을 식별하는 데이터 구조를 생성하고 증명한다
306
모니터가 증명서 및 모니터 키를 봉인한다
308
모니터가 SE 환경을 제거한다
310
모니터가 운영 체제에 제어를 전달하고 복귀 정보를 제공한다
312
운영체제가 웨이크 프로세스를 위해 복귀 정보를 저장한다
314
요구된 휴면 상태에 들어간다
302
휴면 상태

도면4


웨이크 이벤트
휴면 제어기가 웨이크 동작을 수행한다 400
운영체제가 웨이크 동작을 수행한다 402
SE 환경을 복원? 404
아니오
예
운영체제가 모니터를 로딩하고 그 실행을 호출한다 406
모니터가 봉인된 증명서 및 모니터 키를 봉인 해제한다 408
봉인 해제 동작 실패? 410
예
아니오
데이터 구조가 신빙성이 있나? 414
아니오
예
봉인 해제된 모니터 키를 사용하여 메모리 내용을 해독한다 416
내용이 신빙성이 있나? 418
예
아니오
웨이크 상태
휴면 공격 응답 호출 412
종료