(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2016-0111455
(43) 공개일자 2016년09월26일

(51) 국제특허분류(Int. Cl.)
G06F 21/57 (2013.01) *H04L 9/08* (2006.01)
(52) CPC특허분류
G06F 21/575 (2013.01)
H04L 9/0866 (2013.01)
(21) 출원번호 10-2016-7022517
(22) 출원일자(국제) 2015년01월20일
심사청구일자 없음
(85) 번역문제출일자 2016년08월18일
(86) 국제출원번호 PCT/US2015/011991
(87) 국제공개번호 WO 2015/112479
국제공개일자 2015년07월30일
(30) 우선권주장
14/161,185 2014년01월22일 미국(US)

(71) 출원인
퀄컴 인코포레이티드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
라버, 스티븐 더글라스
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
구오, 수
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(뒷면에 계속)
(74) 대리인
특허법인 남앤드남

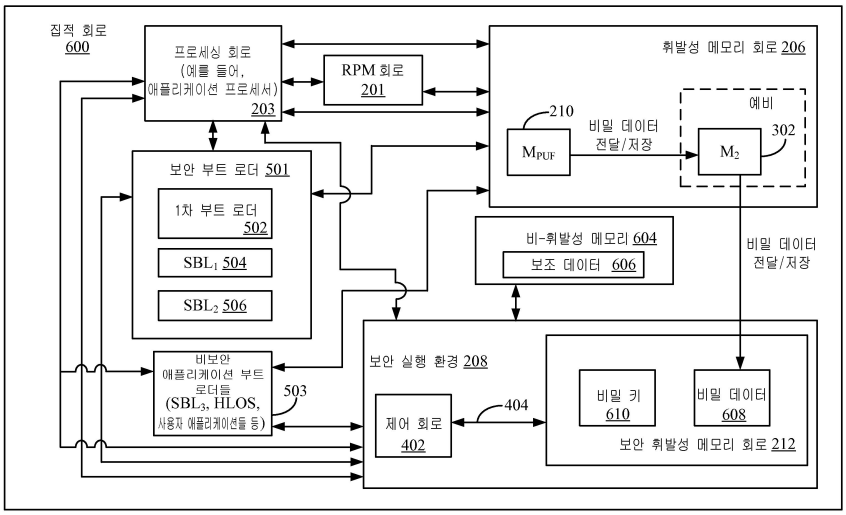
전체 청구항 수 : 총 30 항

(54) 발명의 명칭 **보안 부트 동안 키 추출**

(57) 요 약

하나의 특징은 집적 회로의 보안 부트 흐름 동안 비밀 키를 추출하기 위한 방법에 관련된다. 구체적으로, 보안 부트 흐름은 복수의 초기 로직 상태 값들을 생성하기 위해서 제 1 휘발성 메모리 회로를 파워 온하는 것, 복수의 초기 로직 상태 값들에 기초하여 비밀 데이터를 유추하는 것, 보안 휘발성 메모리 회로에 비밀 데이터를 저장하는 것 – 보안 휘발성 메모리 회로는 SEE(secure execution environment)에 의해 보안됨 –, 제 1 휘발성 메모리 회로에서 복수의 초기 로직 상태 값들을 클리어하는 것, 비밀 데이터에 기초하여 비밀 키를 추출하기 위해서 SEE에서 암호 알고리즘을 실행하는 것, 및 보안 휘발성 메모리 회로에 비밀 키를 저장하는 것을 포함한다. 보안 부트 흐름은 비보안 애플리케이션들로부터 비밀 데이터 및 복수의 초기 로직 상태 값들을 보안하기 위해서 제 1 휘발성 메모리 회로로의 액세스를 제어한다.

대 표 도 - 도6



(52) CPC특허분류
H04L 9/0894 (2013.01)
(72) 발명자
로젠버그, 브라이언 마르크
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
제이콥슨, 데이비드 메릴
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775

명 세 서

청구범위

청구항 1

집적 회로에서의 동작 방법으로서,

복수의 초기 로직 상태 값들을 생성하기 위해서 제 1 휘발성 메모리 회로를 파워 온하는 단계 - 상기 제 1 휘발성 메모리 회로는 상기 집적 회로 상에 있음 - ;

상기 복수의 초기 로직 상태 값들에 기초하여 비밀 데이터를 유추하는 단계;

보안 휘발성 메모리 회로에 상기 비밀 데이터를 저장하는 단계 - 상기 보안 휘발성 메모리 회로는 SEE(secure execution environment)에 의해 보안됨 - ;

상기 제 1 휘발성 메모리 회로에서 복수의 초기 로직 상태 값들을 클리어하는 단계;

상기 비밀 데이터에 기초하여 비밀 키를 추출하기 위해서 상기 SEE에서 암호 알고리즘을 실행하는 단계; 및

상기 보안 휘발성 메모리 회로에 상기 비밀 키를 저장하는 단계를 포함하는,

집적 회로에서의 동작 방법.

청구항 2

제 1 항에 있어서,

상기 방법은 하나 또는 그 초과의 비보안 애플리케이션들로부터 상기 비밀 데이터 및 상기 복수의 초기 로직 상태 값들을 보안하기 위해서 상기 제 1 휘발성 메모리 회로로의 액세스를 제어하는 상기 집적 회로의 보안 부트 흐름인,

집적 회로에서의 동작 방법.

청구항 3

제 2 항에 있어서,

상기 보안 부트 흐름은 적어도 상기 복수의 초기 로직 상태 값들이 상기 제 1 휘발성 메모리 회로에서 클리어된 이후까지 상기 하나 또는 그 초과의 비보안 애플리케이션들에 액세스 불가능한 상기 제 1 휘발성 메모리 회로를 렌더링함으로써 상기 하나 또는 그 초과의 비보안 애플리케이션들로부터 상기 비밀 데이터 및 상기 복수의 초기 로직 상태 값들을 보안하는,

집적 회로에서의 동작 방법.

청구항 4

제 3 항에 있어서,

상기 보안 부트 흐름은 1차 부트 로더, 제 1 2차 부트 로더 및 제 2 2차 부트 로더를 포함하고,

상기 보안 부트 흐름은 상기 제 1 2차 부트 로더가 실행되기 전에 상기 1차 부트 로더가 상기 제 1 2차 부트 로더를 인증하게 하고, 상기 제 2 2차 부트 로더가 실행되기 전에 상기 제 1 2차 부트 로더가 상기 제 2 2차 부트 로더를 인증하게 하고, 상기 제 2 2차 부트 로더가 상기 SEE를 인증하게 함으로써 일련의 신뢰를 설정하고,

상기 비밀 키는 상기 하나 또는 그 초과의 비보안 애플리케이션들의 실행 전에 그리고 상기 보안 부트 흐름 동안 추출되어 상기 보안 휘발성 메모리 회로에 저장되는,

집적 회로에서의 동작 방법.

청구항 5

제 2 항에 있어서,

상기 제 1 휘발성 메모리 회로를 리셋하는 것은 상기 보안 부트 흐름으로 하여금 실행되게 하는,

집적 회로에서의 동작 방법.

청구항 6

제 1 항에 있어서,

상기 비밀 데이터는 상기 복수의 초기 로직 상태 값들인,

집적 회로에서의 동작 방법.

청구항 7

제 1 항에 있어서,

상기 제 1 휘발성 메모리 회로를 클리어한 이후, 상기 제 1 휘발성 메모리 회로는 하나 또는 그 초과의 비보안 애플리케이션들에 대한 데이터 저장에 이용가능한,

집적 회로에서의 동작 방법.

청구항 8

제 1 항에 있어서,

상기 제 1 휘발성 메모리 회로는 SRAM(static random access memory)인,

집적 회로에서의 동작 방법.

청구항 9

제 1 항에 있어서,

상기 SEE는 비보안 애플리케이션들이 상기 보안 휘발성 메모리 회로에 액세스하는 것을 방지하는,

집적 회로에서의 동작 방법.

청구항 10

제 1 항에 있어서,

상기 복수의 초기 로직 상태 값들은 상기 제 1 휘발성 메모리 회로가 파워 온될 때마다 실질적으로 동일한,

집적 회로에서의 동작 방법.

청구항 11

제 1 항에 있어서,

상기 암호 알고리즘은 블록 코드 알고리즘, 확산 코드 알고리즘 및/또는 반복 코드 알고리즘 중 적어도 하나에 기초하는,

집적 회로에서의 동작 방법.

청구항 12

제 1 항에 있어서,

상기 보안 휘발성 메모리 회로에 상기 비밀 데이터를 저장하기 전에 제 2 휘발성 메모리 회로에 상기 비밀 데이터를 저장하는 단계; 및

상기 보안 휘발성 메모리 회로에 상기 비밀 데이터를 저장한 이후 상기 제 2 휘발성 메모리 회로에 저장된 상기 비밀 데이터를 클리어하는 단계를 더 포함하는,

집적 회로에서의 동작 방법.

청구항 13

제 12 항에 있어서,

상기 제 2 휘발성 메모리 회로에 저장된 상기 비밀 데이터를 클리어한 이후, 상기 제 2 휘발성 메모리 회로는 하나 또는 그 초과의 비보안 애플리케이션들에 대한 데이터 저장에 이용가능한,

집적 회로에서의 동작 방법.

청구항 14

제 1 항에 있어서,

상기 SEE는 상기 비밀 키를 비보안 애플리케이션에 액세스 불가능하게 함으로써 상기 비밀 키로의 액세스를 제어하고,

상기 방법은,

2차 키 및/또는 공개 데이터 중 적어도 하나에 대한 SEE에서 상기 비보안 애플리케이션으로부터 요청을 수신하는 단계;

상기 비밀 키에 기초하여 상기 SEE에서 상기 2차 키 및/또는 상기 공개 데이터를 생성하는 단계; 및

상기 2차 키 및/또는 상기 공개 데이터를 요청하는 상기 비보안 애플리케이션에 상기 2차 키 및/또는 상기 공개 데이터를 제공하는 단계를 더 포함하는,

집적 회로에서의 동작 방법.

청구항 15

제 14 항에 있어서,

상기 2차 키 및/또는 상기 공개 데이터는 상기 비보안 애플리케이션에 의해 제공되는 상기 비밀 키 및 다른 데이터에 기초하여 생성되는,

집적 회로에서의 동작 방법.

청구항 16

제 1 항에 있어서,

상기 비밀 데이터에 기초하여 상기 비밀 키를 추출하기 위해서 상기 SEE에서 실행되는 상기 암호 알고리즘은 비-휘발성 메모리 회로에 저장된 보조 데이터에 추가로 기초하는,

집적 회로에서의 동작 방법.

청구항 17

집적 회로로서,

파워 온 시 복수의 초기 로직 상태 값들을 생성하도록 구성되는 제 1 휘발성 메모리 회로;

SEE(secure execution environment)에 의해 보안되는 보안 휘발성 메모리 회로; 및

상기 제 1 휘발성 메모리 회로 및 상기 보안 휘발성 메모리 회로에 통신가능하게 커플링된 프로세싱 회로를 포함하고,

상기 프로세싱 회로는,

상기 복수의 초기 로직 상태 값들에 기초하여 비밀 데이터를 유추하고,

상기 보안 휘발성 메모리 회로에 상기 비밀 데이터를 저장하고,

상기 제 1 휘발성 메모리 회로에서 상기 복수의 초기 로직 상태 값들을 클리어하고,

상기 비밀 데이터에 기초하여 비밀 키를 추출하기 위해서 상기 SEE에서 암호 알고리즘을 실행하고, 그리고

상기 보안 휘발성 메모리 회로에 상기 비밀 키를 저장하도록 구성되는,

집적 회로.

청구항 18

제 17 항에 있어서,

상기 프로세싱 회로는 (i) 상기 비밀 데이터를 유추하고, (ii) 상기 비밀 데이터를 저장하고, (iii) 상기 복수의 초기 로직 상태 값들을 클리어하고, (iv) 상기 암호 알고리즘을 실행시키고, 그리고 (v) 상기 비밀 키를 저장함으로써 보안 부트 흐름을 실행시키고,

상기 보안 부트 흐름은 하나 또는 그 초과의 비보안 애플리케이션들로부터 상기 비밀 데이터 및 상기 복수의 초기 로직 상태 값들을 보안하기 위해서 상기 제 1 휘발성 메모리 회로로의 액세스를 제어하는,

집적 회로.

청구항 19

제 18 항에 있어서,

상기 보안 부트 흐름은 적어도 상기 복수의 초기 로직 상태 값들이 상기 제 1 휘발성 메모리 회로에서 클리어된 이후까지 상기 하나 또는 그 초과의 비보안 애플리케이션들에 액세스 불가능한 상기 제 1 휘발성 메모리 회로를 렌더링함으로써 상기 하나 또는 그 초과의 비보안 애플리케이션들로부터 상기 비밀 데이터 및 상기 복수의 초기 로직 상태 값들을 보안하는,

집적 회로.

청구항 20

제 19 항에 있어서,

상기 보안 부트 흐름은 1차 부트 로더, 제 1 2차 부트 로더 및 제 2 2차 부트 로더를 포함하고,

상기 보안 부트 흐름은 상기 제 1 2차 부트 로더가 실행되기 전에 상기 1차 부트 로더가 상기 제 1 2차 부트 로더를 인증하게 하고, 상기 제 2 2차 부트 로더가 실행되기 전에 상기 제 1 2차 부트 로더가 상기 제 2 2차 부트 로더를 인증하게 하고, 상기 제 2 2차 부트 로더가 상기 SEE를 인증하게 함으로써 일련의 신뢰를 설정하고,

상기 비밀 키는 상기 하나 또는 그 초과의 비보안 애플리케이션들의 실행 전에 그리고 상기 보안 부트 흐름 동안 추출되어 상기 보안 휘발성 메모리 회로에 저장되는,

집적 회로.

청구항 21

제 18 항에 있어서,

상기 제 1 휘발성 메모리 회로를 리셋하는 것은 상기 보안 부트 흐름으로 하여금 실행되게 하는,

집적 회로.

청구항 22

제 17 항에 있어서,

상기 제 1 휘발성 메모리 회로를 클리어한 이후, 상기 제 1 휘발성 메모리 회로는 하나 또는 그 초과의 비보안 애플리케이션들에 대한 데이터 저장에 이용가능한,

집적 회로.

청구항 23

제 17 항에 있어서,

상기 프로세싱 회로는,

상기 보안 휘발성 메모리 회로에 상기 비밀 데이터를 저장하기 전에 제 2 휘발성 메모리 회로에 상기 비밀 데이터를 저장하고, 그리고

상기 보안 휘발성 메모리 회로에 상기 비밀 데이터를 저장한 이후 상기 제 2 휘발성 메모리 회로에 저장된 상기 비밀 데이터를 클리어하도록 추가로 구성되는,

집적 회로.

청구항 24

제 17 항에 있어서,

상기 SEE는 상기 비밀 키를 비보안 애플리케이션에 액세스 불가능하게 함으로써 상기 비밀 키로의 액세스를 제어하고,

상기 프로세싱 회로는,

2차 키 및/또는 공개 데이터 중 적어도 하나에 대한 SEE에서 상기 비보안 애플리케이션으로부터 요청을 수신하고;

상기 비밀 키에 기초하여 상기 SEE에서 상기 2차 키 및/또는 상기 공개 데이터를 생성하고; 그리고

상기 2차 키 및/또는 상기 공개 데이터를 요청하는 상기 비보안 애플리케이션에 상기 2차 키 및/또는 상기 공개 데이터를 제공하도록 추가로 구성되는,

집적 회로.

청구항 25

제 17 항에 있어서,

상기 비밀 데이터에 기초하여 상기 비밀 키를 추출하기 위해서 상기 SEE에서 실행되는 상기 암호 알고리즘은 비-휘발성 메모리 회로에 저장된 보조 데이터에 추가로 기초하는,

집적 회로.

청구항 26

집적 회로로서,

복수의 초기 로직 상태 값들을 생성하기 위해서 제 1 휘발성 메모리 회로를 파워 온하기 위한 수단 - 상기 제 1 휘발성 메모리 회로는 상기 집적 회로 상에 있음 - ;

상기 복수의 초기 로직 상태 값들에 기초하여 비밀 데이터를 유추하기 위한 수단;

보안 휘발성 메모리 회로에 상기 비밀 데이터를 저장하기 위한 수단 - 상기 보안 휘발성 메모리 회로는 SEE(secure execution environment)에 의해 보안됨 - ;

상기 제 1 휘발성 메모리 회로에서 복수의 초기 로직 상태 값들을 클리어하기 위한 수단;

상기 비밀 데이터에 기초하여 비밀 키를 추출하기 위해서 상기 SEE에서 암호 알고리즘을 실행하기 위한 수단; 및

상기 보안 휘발성 메모리 회로에 상기 비밀 키를 저장하기 위한 수단을 포함하는,

집적 회로.

청구항 27

제 26 항에 있어서,

상기 제 1 휘발성 메모리 회로로의 액세스는 적어도 상기 복수의 초기 로직 상태 값들이 상기 제 1 휘발성 메모

리 회로에서 클리어된 이후까지 상기 하나 또는 그 초과의 비보안 애플리케이션들에 액세스 불가능한 상기 제 1 휘발성 메모리 회로를 렌더링함으로써 상기 하나 또는 그 초과의 비보안 애플리케이션들로부터 상기 비밀 데이터 및 상기 복수의 초기 로직 상태 값들을 보안하도록 제어되는,

집적 회로.

청구항 28

제 27 항에 있어서,

상기 제 1 휘발성 메모리 회로를 리셋하는 것은 상기 집적 회로로 하여금 리셋되어 보안 부트 흐름을 겪게 하는,

집적 회로.

청구항 29

하나 또는 그 초과의 명령들을 갖는 컴퓨터 판독가능한 저장 매체로서,

상기 명령들은, 적어도 하나의 집적 회로에 의해 실행될 때, 상기 집적 회로로 하여금,

복수의 초기 로직 상태 값들을 생성하기 위해서 제 1 휘발성 메모리 회로를 파워 온하게 하고 - 상기 제 1 휘발성 메모리 회로는 상기 집적 회로 상에 있음 - ;

상기 복수의 초기 로직 상태 값들에 기초하여 비밀 데이터를 유추하게 하고;

보안 휘발성 메모리 회로에 상기 비밀 데이터를 저장하게 하고 - 상기 보안 휘발성 메모리 회로는 SEE(secure execution environment)에 의해 보안됨 - ;

상기 제 1 휘발성 메모리 회로에서 복수의 초기 로직 상태 값들을 클리어하게 하고;

상기 비밀 데이터에 기초하여 비밀 키를 추출하기 위해서 상기 SEE에서 암호 알고리즘을 실행하게 하고; 그리고

상기 보안 휘발성 메모리 회로에 상기 비밀 키를 저장하게 하는,

컴퓨터 판독가능한 저장 매체.

청구항 30

제 29 항에 있어서,

상기 하나 또는 그 초과의 명령들은 상기 집적 회로의 보안 부트 흐름을 위한 것이고,

상기 명령들은 상기 집적 회로에 의해 실행될 때, 상기 제 1 휘발성 메모리 회로로의 액세스로 하여금, 적어도 상기 복수의 초기 로직 상태 값들이 상기 제 1 휘발성 메모리 회로에서 클리어된 이후까지 상기 하나 또는 그 초과의 비보안 애플리케이션들에 액세스 불가능한 상기 제 1 휘발성 메모리 회로를 렌더링함으로써 하나 또는 그 초과의 비보안 애플리케이션들로부터 상기 비밀 데이터 및 상기 복수의 초기 로직 상태 값들을 보안하도록 제어되게 하는,

컴퓨터 판독가능한 저장 매체.

발명의 설명

기 술 분 야

[0001] [0001] 본 출원은 2014년 1월 22일자로 미국 특허청에 출원된 미국 정규 특허 출원 번호 제14/161,185호에 대한 우선권 및 이익을 주장하며, 상기 특허 출원의 전체 내용은 인용에 의해 본원에 포함된다.

[0002] [0002] 다양한 특징들은 일반적으로 보안 암호 키 추출 및 저장에 관한 것으로, 더 구체적으로는, 휘발성 메모리의 물리적으로 복제 불가능한(unclonable) 특징들에 기초하여 보안 부트 프로세스 동안 비밀 암호 키를 추출 및 저장하는 것에 관한 것이다.

배 경 기 술

[0003] [0003] 모바일 폰들, 태블릿들 및 컴퓨터들과 같은 많은 전자 통신 디바이스들은 전자 통신 디바이스에서의 암호 보안 프로세스들에 대해 사용될 수 있는 디바이스-특정 암호 키(또는 이러한 키로부터 유추되는 키들)를 포함한다. 예를 들어, 단지 디바이스에 그리고 가능하게는 또 다른 신뢰성 있는 엔티티(예를 들어, 통신 서비스를 디바이스에 제공하는 셀룰러 네트워크 인증 서버)에 공지된 디바이스-특정 키는 디바이스에 의해 송신되는 통신 메시지들을 암호화하는데 후속적으로 사용되는 키들(예를 들어, 공개-개인 키 페어)을 유추하는데 사용된다. 다른 당사자들(parties) 및/또는 애플리케이션들에 의해 허가되지 않은 액세스로부터의 디바이스-특정 키를 보안하는 것은 디바이스 및/또는 통신 네트워크에 의해 이용되는 암호 보안 프로토콜들의 무결성을 더 양호하게 보장하기 위해서 최고의 중요성을 갖는다.

[0004] [0004] 도 1은 전자 통신 디바이스에서 발견될 수 있는 종래 기술 IC(integrated circuit)(100)의 개략 블록도를 예시한다. IC(100)는 부트 로더(102), 사용자 애플리케이션들(104) 및 비-휘발성 메모리 회로(106)를 포함하며, 이는 결국 IC(100)를 갖는 디바이스에 고유할 수 있는 암호 키(108)를 저장한다. IC(100)가 파워 온될 때, IC(100)는 IC(100)의 다양한 양상들을 초기화하는 부트 로더를 리트리브 및 실행시킨다. IC(100)가 자신의 부트 업 프로세스를 완료한 이후, 사용자 애플리케이션들(104)(예를 들어, HLOS(high level operating systems), 이러한 HLOS 상에서 실행되는 애플리케이션들 등)이 실행될 수 있다. 부트 로더(102) 및 사용자 애플리케이션들(104)은 키(108)로의 다이렉트 액세스를 가질 수 있다. 예를 들어, 사용자 애플리케이션은 비-휘발성 메모리(106)로부터 키(108)를 리트리브하고, 그것을 사용하여 암호 프로세스들에 대해 사용되는 추가 키들을 유추할 수 있다.

[0005] [0005] 더욱이, 키(108)를 저장하는 메모리 회로(106)는 비-휘발성 메모리이기 때문에, 키(108)는 IC(100)가 파워 오프되는지 아니면 파워 온되는지에 관계없이 IC(100)에 저장된다(따라서, 이론상으로 액세스가능함). 이것은 키(108)를 더 큰 보안 취약성에 노출시킨다. 예를 들어, 집적 회로(100) 패키지의 상단은 물리적으로 개방될 수 있고, 전자 현미경은 키(108)를 저장하기 위해서 사용되는 회로(예를 들어, 퓨즈들)를 분석하는데 사용될 수 있다. 그렇게 하는 것은 키(108)를 드러내고, 디바이스의 보안을 절충할 수 있다.

[0006] [0006] 이러한 키들로의 허가되지 않은 액세스를 방지하는 것을 돕기 위해서 키 추출/생성 및 저장에서 증가되는 보안을 제공하는 방법들 및 장치들에 대한 필요성이 존재한다. 키 추출/생성 및 저장에서의 개선된 보안은 이러한 키들에 의존하는 암호 알고리즘들 및 프로세스들의 신뢰도 및 신뢰성을 증가시키는 것을 돕는다.

발명의 내용

[0007] [0007] 하나의 특징은 집적 회로에서 동작가능한 방법을 제공하고, 방법은, 복수의 초기 로직 상태 값들을 생성하기 위해서 제 1 휘발성 메모리 회로를 파워 온하는 단계 - 제 1 휘발성 메모리 회로는 집적 회로 상에 있음 - , 복수의 초기 로직 상태 값들에 기초하여 비밀 데이터를 유추하는 단계, 보안 휘발성 메모리 회로에 비밀 데이터를 저장하는 단계 - 보안 휘발성 메모리 회로는 SEE(secure execution environment)에 의해 보안됨 - , 제 1 휘발성 메모리 회로에서 복수의 초기 로직 상태 값들을 클리어하는 단계, 비밀 데이터에 기초하여 비밀 키를 추출하기 위해서 SEE에서 암호 알고리즘을 실행하는 단계, 및 보안 휘발성 메모리 회로에 비밀 키를 저장하는 단계를 포함한다. 하나의 양상에 따라, 방법은 하나 또는 그 초과의 비보안 애플리케이션들로부터 비밀 데이터 및 복수의 초기 로직 상태 값들을 보안하기 위해서 제 1 휘발성 메모리 회로로의 액세스를 제어하는 집적 회로의 보안 부트 흐름이다. 또 다른 양상에 따라, 보안 부트 흐름은 적어도 복수의 초기 로직 상태 값들이 제 1 휘발성 메모리 회로에서 클리어된 이후까지 하나 또는 그 초과의 비보안 애플리케이션들에 액세스 불가능한 제 1 휘발성 메모리 회로를 렌더링함으로써 하나 또는 그 초과의 비보안 애플리케이션들로부터 비밀 데이터 및 복수의 초기 로직 상태 값들을 보안한다.

[0008] [0008] 하나의 양상에 따라, 보안 부트 흐름은 1차 부트 로더, 제 1 2차 부트 로더 및 제 2 2차 부트 로더를 포함하고, 보안 부트 흐름은 제 1 2차 부트 로더가 실행되기 전에 1차 부트 로더가 제 1 2차 부트 로더를 인증하게 하고, 제 2 2차 부트 로더가 실행되기 전에 제 1 2차 부트 로더가 제 2 2차 부트 로더를 인증하게 하고, 제 2 2차 부트 로더가 SEE를 인증하게 함으로써 일련의 신뢰를 설정하고, 비밀 키는 하나 또는 그 초과의 비보안 애플리케이션들의 실행 전에 그리고 보안 부트 흐름 동안 추출되어 보안 휘발성 메모리 회로에 저장된다. 또 다른 양상에 따라, 제 1 휘발성 메모리 회로를 리셋하는 것은 보안 부트 흐름으로 하여금 실행되게 한다. 또 다른 양상에 따라, 비밀 데이터는 복수의 초기 로직 상태 값들이다.

[0009] [0009] 하나의 양상에 따라, 제 1 휘발성 메모리 회로를 클리어한 이후, 제 1 휘발성 메모리 회로는 하나 또는 그 초과의 비보안 애플리케이션들에 대한 데이터 저장에 이용가능하다. 또 다른 양상에 따라, 제 1 휘발성 메

모리 회로는 SRAM(static random access memory)이다. 또 다른 양상에 따라, SEE는 비보안 애플리케이션들이 보안 휘발성 메모리 회로에 액세스하는 것을 방지한다.

[0010] [0010] 하나의 양상에 따라, 복수의 초기 로직 상태 값들은 제 1 휘발성 메모리 회로가 파워 온될 때마다 실질적으로 동일하다 . 또 다른 양상에 따라, 암호 알고리즘은 블록 코드 알고리즘, 확산 코드 알고리즘 및/또는 반복 코드 알고리즘 중 적어도 하나에 기초한다. 또 다른 양상에 따라, 방법은 보안 휘발성 메모리 회로에 비밀 데이터를 저장하기 전에 제 2 휘발성 메모리 회로에 비밀 데이터를 저장하는 단계, 및 보안 휘발성 메모리 회로에 비밀 데이터를 저장한 이후 제 2 휘발성 메모리 회로에 저장된 비밀 데이터를 클리어하는 단계를 더 포함한다.

[0011] [0011] 하나의 양상에 따라, 제 2 휘발성 메모리 회로에 저장된 비밀 데이터를 클리어한 이후, 제 2 휘발성 메모리 회로는 하나 또는 그 초과의 비보안 애플리케이션들에 대한 데이터 저장에 이용가능하다. 또 다른 양상에 따라, SEE는 비밀 키를 비보안 애플리케이션에 액세스 불가능하게 함으로써 비밀 키로의 액세스를 제어하고, 방법은 2차 키 및/또는 공개 데이터 중 적어도 하나에 대한 SEE에서 비보안 애플리케이션으로부터 요청을 수신하는 단계, 비밀 키에 기초하여 SEE에서 2차 키 및/또는 공개 데이터를 생성하는 단계, 및 2차 키 및/또는 공개 데이터를 요청하는 비보안 애플리케이션에 2차 키 및/또는 공개 데이터를 제공하는 단계를 더 포함한다. 또 다른 양상에 따라, 2차 키 및/또는 공개 데이터는 비보안 애플리케이션에 의해 제공되는 비밀 키 및 다른 데이터에 기초하여 생성된다. 또 다른 양상에 따라, 비밀 데이터에 기초하여 비밀 키를 추출하기 위해서 SEE에서 실행되는 암호 알고리즘은 비-휘발성 메모리 회로에 저장된 보조 데이터에 추가로 기초한다.

[0012] [0012] 또 다른 특징은 파워 온 시 복수의 초기 로직 상태 값들을 생성하도록 구성되는 제 1 휘발성 메모리 회로, SEE(secure execution environment)에 의해 보안되는 보안 휘발성 메모리 회로, 및 제 1 휘발성 메모리 회로 및 보안 휘발성 메모리 회로에 통신가능하게 커플링된 프로세싱 회로를 포함하는 집적 회로를 제공하고, 프로세싱 회로는 복수의 초기 로직 상태 값들에 기초하여 비밀 데이터를 유추하고, 보안 휘발성 메모리 회로에 비밀 데이터를 저장하고, 제 1 휘발성 메모리 회로에서 복수의 초기 로직 상태 값들을 클리어하고, 비밀 데이터에 기초하여 비밀 키를 추출하기 위해서 SEE에서 암호 알고리즘을 실행하고, 그리고 보안 휘발성 메모리 회로에 비밀 키를 저장하도록 구성된다. 하나의 양상에 따라, 프로세싱 회로는 (i) 비밀 데이터를 유추하고, (ii) 비밀 데이터를 저장하고, (iii) 복수의 초기 로직 상태 값들을 클리어하고, (iv) 암호 알고리즘을 실행시키고, 그리고 (v) 비밀 키를 저장함으로써 보안 부트 흐름을 실행시키고, 보안 부트 흐름은 하나 또는 그 초과의 비보안 애플리케이션들로부터 비밀 데이터 및 복수의 초기 로직 상태 값들을 보안하기 위해서 제 1 휘발성 메모리 회로로의 액세스를 제어한다.

[0013] [0013] 하나의 양상에 따라, 프로세싱 회로는 보안 휘발성 메모리 회로에 비밀 데이터를 저장하기 전에 제 2 휘발성 메모리 회로에 비밀 데이터를 저장하고, 그리고 보안 휘발성 메모리 회로에 비밀 데이터를 저장한 이후 제 2 휘발성 메모리 회로에 저장된 비밀 데이터를 클리어하도록 추가로 구성된다. 또 다른 양상에 따라, SEE는 비밀 키를 비보안 애플리케이션에 액세스 불가능하게 함으로써 비밀 키로의 액세스를 제어하고, 프로세싱 회로는 2차 키 및/또는 공개 데이터 중 적어도 하나에 대한 SEE에서 비보안 애플리케이션으로부터 요청을 수신하고, 비밀 키에 기초하여 SEE에서 2차 키 및/또는 공개 데이터를 생성하고, 그리고 2차 키 및/또는 공개 데이터를 요청하는 비보안 애플리케이션에 2차 키 및/또는 공개 데이터를 제공하도록 추가로 구성된다.

[0014] [0014] 또 다른 특징은 복수의 초기 로직 상태 값들을 생성하기 위해서 제 1 휘발성 메모리 회로를 파워 온하기 위한 수단 - 제 1 휘발성 메모리 회로는 집적 회로 상에 있음 - , 복수의 초기 로직 상태 값들에 기초하여 비밀 데이터를 유추하기 위한 수단, 보안 휘발성 메모리 회로에 비밀 데이터를 저장하기 위한 수단 - 보안 휘발성 메모리 회로는 SEE(secure execution environment)에 의해 보안됨 - , 제 1 휘발성 메모리 회로에서 복수의 초기 로직 상태 값들을 클리어하기 위한 수단, 비밀 데이터에 기초하여 비밀 키를 추출하기 위해서 SEE에서 암호 알고리즘을 실행하기 위한 수단, 및 보안 휘발성 메모리 회로에 비밀 키를 저장하기 위한 수단을 포함하는 집적 회로를 제공한다.

[0015] [0015] 또 다른 특징은 하나 또는 그 초과의 명령들을 갖는 컴퓨터 판독가능한 저장 매체를 제공하며, 명령들은, 적어도 하나의 집적 회로에 의해 실행될 때, 집적 회로로 하여금, 복수의 초기 로직 상태 값들을 생성하기 위해서 제 1 휘발성 메모리 회로를 파워 온하게 하고 - 제 1 휘발성 메모리 회로는 집적 회로 상에 있음 - , 복수의 초기 로직 상태 값들에 기초하여 비밀 데이터를 유추하게 하고; 보안 휘발성 메모리 회로에 비밀 데이터를 저장하게 하고 - 보안 휘발성 메모리 회로는 SEE(secure execution environment)에 의해 보안됨 - , 제 1 휘발성 메모리 회로에서 복수의 초기 로직 상태 값들을 클리어하게 하고, 비밀 데이터에 기초하여 비

밀 키를 추출하기 위해서 SEE에서 암호 알고리즘을 실행하게 하고, 그리고 보안 휘발성 메모리 회로에 비밀 키를 저장하게 한다. 하나의 양상에 따라, 하나 또는 그 초과의 명령들은 집적 회로의 보안 부트 흐름을 위한 것이고, 명령들은 집적 회로에 의해 실행될 때, 제 1 휘발성 메모리 회로로의 액세스로 하여금, 적어도 복수의 초기 로직 상태 값들이 제 1 휘발성 메모리 회로에서 클리어된 이후까지 하나 또는 그 초과의 비보안 애플리케이션들에 액세스 불가능한 제 1 휘발성 메모리 회로를 렌더링함으로써 하나 또는 그 초과의 비보안 애플리케이션들로부터 비밀 데이터 및 복수의 초기 로직 상태 값들을 보안하도록 제어되게 한다.

도면의 간단한 설명

[0016] [0016] 도 1은 전자 통신 디바이스에서 발견될 수 있는 종래 기술의 IC(integrated circuit)의 개략 블록도를 예시한다.

[0017] 도 2는 IC의 하이 레벨 개략 블록도를 예시한다.

[0018] 도 3은 휘발성 메모리 회로의 개략 블록도를 예시한다.

[0019] 도 4는 보안 실행 환경의 개략 블록도를 예시한다.

[0020] 도 5는 보안 부트 흐름 계층을 예시한다.

[0021] 도 6은 비밀 키를 추출하여 저장하는 보안 부트 흐름을 특징화하는 IC를 예시한다.

[0022] 도 7a 및 도 7b를 포함하는 도 7은 집적 회로로 하여금 비밀 키를 추출하여 저장하게 하는 보안 부트 흐름을 도시하는 흐름도를 예시한다.

[0023] 도 8은 집적 회로에서 동작가능한 방법을 예시한다.

[0024] 도 9는 본원에서 설명되는 IC들의 프로세싱 회로의 개략 블록도를 예시한다.

발명을 실시하기 위한 구체적인 내용

[0017] [0025] 다음의 설명에서, 특정 세부사항들은 본 개시 내용의 다양한 양상들의 철저한 이해를 제공하기 위해서 주어진다. 그러나, 양상들이 이러한 특정 세부사항들 없이 실시될 수 있다는 것이 당업자에 의해 이해될 것이다. 예를 들어, 회로들은 불필요하게 상설하여 양상들을 모호하게 하는 것을 회피하기 위해서 블록도들로 도시될 수 있다. 다른 예들에서, 잘-알려져 있는 회로들, 구조들 및 기법들은 본 개시 내용의 양상들을 모호하게 하지 않기 위해서 상세하게 도시되지 않을 수 있다.

[0018] [0026] "예시적"이라는 단어는 본원에서 "예, 예시 또는 예증으로서 제공되는"의 의미로 사용된다. "예시적"으로서 본원에서 설명되는 임의의 구현 또는 양상이 반드시 본 개시 내용의 다른 양상들보다 선호되거나 또는 유리한 것으로 해석되는 것은 아니다. 마찬가지로, "양상들"이라는 용어는, 본 개시 내용의 모든 양상들이 논의되는 특징, 이점 또는 동작 모드를 포함하는 것을 요구하지 않는다.

[0019] **개요**

[0020] [0027] 집적 회로의 보안 부트 흐름 동안 비밀 키를 추출하는 방법들 및 장치들이 본원에서 설명된다. 구체적으로, 보안 부트 흐름은 복수의 초기 로직 상태 값들을 생성하기 위해서 제 1 휘발성 메모리 회로를 파워 온하는 것, 복수의 초기 로직 상태 값들에 기초하여 비밀 데이터를 유추하는 것, 보안 휘발성 메모리 회로에 비밀 데이터를 저장하는 것 – 보안 휘발성 메모리 회로는 SEE(secure execution environment)에 의해 보안됨 – , 제 1 휘발성 메모리 회로에서 복수의 초기 로직 상태 값들을 클리어하는 것, 비밀 데이터에 기초하여 비밀 키를 추출하기 위해서 SEE에서 암호 알고리즘을 실행하는 것, 및 보안 휘발성 메모리 회로에 비밀 키를 저장하는 것을 포함한다. 보안 부트 흐름은 적어도 복수의 초기 로직 상태 값들이 제 1 휘발성 메모리 회로에서 클리어된 이후까지 비보안 애플리케이션들에 액세스 불가능한 제 1 휘발성 메모리 회로를 렌더링함으로써 비보안 애플리케이션들로부터 비밀 데이터 및 복수의 초기 로직 상태 값들을 보안하도록 제 1 휘발성 메모리 회로로의 액세스를 제어한다. 더욱이, 제 1 휘발성 메모리 회로가 리셋되면, 보안 부트 흐름이 다시 개시되고, 따라서, 제 1 휘발성 메모리 회로의 초기 로직 상태 값들은 비보안 애플리케이션들에 이용가능하지 않다.

[0021] **IC 보안 부트 업 동안의 예시적 키 추출**

[0022] [0028] 도 2는 본 개시 내용의 하나의 양상에 따른 IC(integrated circuit)(200)의 하이 레벨 개략 블록도를 예시한다. IC(200)는, 예를 들어, 프로세싱 회로들, 메모리 회로들 등을 포함하는 프로세서일 수 있으며, 모바

일 폰, 컴퓨터, 태블릿, 시계 등과 같은(그러나, 이들에 제한되는 것은 아님) 전자 통신 디바이스에서 발견될 수 있다. IC(200)는 RPM(resource power management) 회로(201), 보안 부트 로더 회로(202), 프로세싱 회로(203), 비보안 애플리케이션들(204), 휘발성 메모리 회로(206) 및 SEE(secure execution environment)(208)를 포함할 수 있다. 휘발성 메모리 회로(206)는 PUF(physically unclonable function)(210)를 포함하고, SEE(208)는 보안 휘발성 메모리 회로(212)를 포함한다.

[0023] [0029] 그 중에서도, RPM 회로(201)는 IC(200)의 다양한 회로들 및 컴포넌트들에 파워를 공급한다. 예를 들어, RPM 회로(201)는 프로세싱 회로(203), 휘발성 메모리 회로(206) 및/또는 보안 휘발성 메모리 회로(212)에 공급되는 파워를 제어할 수 있다. RPM 회로(201)는 복수의 초기 로직 상태 값들을 생성하기 위해서 제 1 휘발성 메모리 회로를 파워 온하기 위한 수단의 하나의 예를 표현한다.

[0024] [0030] IC(200)의 파워 온 시, IC(200)는 프로세싱 회로(203)가 보안 부트 로더(예를 들어, 보안 부트 코드)(202)를 획득하여 실행시키게 함으로써 보안 부트 업 프로세스(본원에서 "보안 부트 흐름"으로 또한 지칭됨)를 겪고/실행시킨다. 보안 부트 로더(202)는 ROM(read-only memory) 및/또는 다른 비-휘발성 메모리와 같은 메모리 회로들(그러나 이들에 제한되는 것은 아님)에 저장될 수 있다. 보안 부트 로더(202)는 IC(200)의 다양한 모듈들을 초기화하며, 정상 동작을 위하여 IC(200)를 준비시키기 위해서 다른 기본 동작들을 수행한다.

[0025] [0031] 본 개시 내용의 하나의 양상에 따라, 휘발성 메모리 회로(206)는 각각이 복수의 SRAM 회로 셀들을 포함하는 하나 또는 그 초과의 SRAM(static random access memory) 회로들을 포함한다. 다른 양상들에 따라, 휘발성 메모리 회로(206)는 SRAM에 제한되는 것은 아니며, eDRAM(embedded dynamic random access memory)과 같은 다른 타입들의 휘발성 메모리에 기초할 수 있다. 휘발성 메모리 회로(206)(즉, 다수의 휘발성 메모리 셀들)의 부분은 PUF(physically unclonable function)의 기본을 형성할 수 있다.

[0026] [0032] 온-칩 PUF는 IC(integrated circuit)들의 프로세스 변형들의 제조를 이용하는 칩-고유 시도-응답(challenge-response) 메커니즘이다. 물리적 자극(즉, 시도)이 PUF에 적용되는 경우, PUF는 PUF를 이용하는 디바이스의 물리적 마이크로구조와의 자극의 복잡한 상호작용에 기인하여 예측 불가능하지만 반복가능한 방식으로 응답을 생성한다. 이러한 정확한 마이크로구조는 PUF를 이용하는 디바이스의 제조 동안 도입되는 물리적 인자들에 의존하며, 이는 예측 불가능하다. PUF의 "복제 불가능성(unclonability)"은 하나의 디바이스가 또 다른 외견상으로 동일한 디바이스와 동일한 프로세스로 제조되는 경우에도, PUF를 이용하는 각각의 디바이스는 응답들에 시도들을 맵핑하는 고유한 그리고 예측 불가능한 방식을 갖는다는 것을 의미한다. 따라서, 제조 프로세스 상에서의 정확한 제어가 실행 불가능하기 때문에, 또 다른 디바이스의 PUF와 동일한 시도-응답 동작을 구성하는 것은 사실상 실행 불가능하다.

[0027] [0033] 본 개시 내용에서, 휘발성 메모리 회로(206)는 휘발성 메모리의 타입(예를 들어, SRAM)이며, 여기서, 휘발성 메모리 회로(206)를 포함하는 각각의 회로 셀은 스타트-업 시(즉, 파워 온될 때) 초기 선호되는 로직 상태 값(예를 들어, "0" 또는 "1")으로 자연적으로 초기화된다. 예를 들어, SRAM은 파워 온될 때 이러한 속성을 갖는다. 각각의 휘발성 메모리 셀은 높은 확률로 스타트-업 시 매번 동일한 값으로 초기화되므로, 회로 셀들의 초기 로직 상태 값들은 반복가능하다. 그러나, 회로 셀들의 초기 로직 상태 값들은, 동일하게 제조되는 경우에도, 하나의 IC로부터 또 다른 IC까지 랜덤하다. 따라서, 프로세스 변형 제조에 기인하여, 각각의 집적 회로의 휘발성 메모리 회로들(206) – 동일하게 제조되는 경우에도 – 은 IC당 초기 휘발성 메모리 회로의 스타트업 값들이 상이한 IC들에 걸쳐 동일한 메모리 어드레스 위치들에서 상이하도록 상이한 반복가능한 초기 값들을 나타낼 것이다. 따라서, 각각의 IC(200)는, 자신의 휘발성 메모리 회로의 셀들의 초기 파워 온 상태들에 기초하여 고유하지만 반복가능한 식별자를 갖는 휘발성 메모리 회로(206)(예를 들어, SRAM 회로)를 갖는다.

[0028] [0034] PUF(210)에 대해 기반으로서 사용되는 휘발성 메모리 회로(206)의 휘발성 메모리 셀들의 부분/수는 애플리케이션에 따라 달라질 수 있다. 하나의 예에 따라, 휘발성 메모리 회로(206)의 8 킬로바이트 부분은 PUF(210)를 포함할 수 있다. 그러나, 실제로, PUF(210)에 대해 사용되는 메모리의 양은 512 바이트들, 1 킬로바이트, 2 킬로바이트들, 4 킬로바이트들, 8 킬로바이트들, 16 킬로바이트들 등과 같은(그러나, 이들에 제한되는 것은 아님) 임의의 값일 수 있다. 전체 휘발성 메모리 회로(206)의 크기는 전형적으로, PUF(210)에 대해 사용되는 부분보다 크다. 하나의 예를 들자면, 휘발성 메모리 회로(206)는 384 킬로바이트들일 수 있다. 그러나, 휘발성 메모리 회로(206)는 64 킬로바이트들, 128 킬로바이트들, 256, 킬로바이트들, 384 킬로바이트들, 512 킬로바이트들, 768 킬로바이트들, 1,024 킬로바이트들, 2,048 킬로바이트들 등과 같은(그러나, 이들에 제한되는 것은 아님) 임의의 크기일 수 있다.

[0029] [0035] 위에서 설명된 바와 같이, 휘발성 메모리 회로(206)가 파워 온될 때, 그것의 메모리 회로 셀들 각각은

셀들 사이의 근소한(minute) 제조 변형에 기초하여 초기에 선호되는 로직 상태 값으로 놓인다. PUF(210)로서 사용되는 메모리의 부분은 전혀 다르지 않다: 그것의 메모리 셀들 또한 선호되는 초기 로직 상태 값들로 초기에 놓일 것이다. 이런 의미에서, PUF 시도는 PUF(210)의 휘발성 메모리 회로 셀들을 파워 온시키는 것으로 고려될 수 있고, 그 응답은 그것의 메모리 회로 셀들의 초기 로직 상태 값이다.

[0030] [0036] 일단 PUF(210)의 메모리 회로 셀들이 자신들의 초기 로직 상태 값으로 놓인다면, 보안 부트 로더(202)는 초기 로직 상태 값들에 기초하여 비밀 데이터를 유추할 수 있다. 하나의 양상에 따라, 비밀 데이터는 초기 로직 상태 값들과 동일할 수 있다. 또 다른 양상에 따라, 비밀 데이터는 초기 로직 상태 값들의 동일한 함수에 기초하여 유추될 수 있다. 비밀 데이터가 기초하는 함수의 일부 비-제한적 예들은: 초기 로직 상태 값들의 모든 다른(또는 일부 다른 다수의) 비트와 동일한 비밀 데이터, 초기 로직 상태 값들에 대해 수행되는 하나 또는 그 초과의 수학적 연산들(가산, 감산, 연접(concatenation) 등)에 기초하는 값과 동일한 비밀 데이터 등을 포함하지만, 이들에 제한되는 것은 아니다. 그 다음, 보안 부트 로더(202)는 SEE(208)에 의해 제어되는 보안 휘발성 메모리 회로(212)에 비밀 데이터를 저장한다. 다음으로, 보안 부트 로더(202)는 PUF(210)의 메모리 회로 셀들의 그들의 초기 로직 상태 값들을 클리어/삭제한다. 그것은 로직 상태 "0" 또는 "1"을 모든 PUF(210)의 메모리 회로 셀들에 기록함으로써 또는 그들의 로직 상태 값들을 랜덤하게 변경(랜덤한 "0" 또는 "1")함으로써 이것을 달성할 수 있다. 유사한 방식으로, 보안 부트 로더(202)는 또한, 보안 휘발성 메모리 회로(212) 외부의 어디엔가 일시적으로 저장될 수 있는 비밀 데이터 중 임의의 것을 클리어/삭제한다. 일단 클리어되면, 초기 로직 상태 값들을 원래 저장하였던 메모리 회로 셀들은 필요에 따라 일반적 데이터 저장에 대해 자유롭게 사용된다. 예를 들어, 일단 HLOS(high level operating system) 및 사용자 애플리케이션들이 로딩 및 실행되면, 그들은 이러한 클리어된 메모리 회로 셀들을 사용할 수 있다.

[0031] [0037] 따라서, 보안 부트 로더(202)는 복수의 초기 로직 상태 값들에 기초하여 비밀 데이터를 유추하기 위한 수단의 하나의 예를 표현한다. 보안 부트 로더(202)는 또한, 보안 휘발성 메모리 회로(212)에 비밀 데이터를 저장하기 위한 수단의 하나의 예를 표현한다. 더욱이, 보안 부트 로더(202)는 제 1 휘발성 메모리 회로(206)에서 복수의 초기 로직 상태 값들을 클리어하기 위한 수단의 하나의 예를 표현한다.

[0032] [0038] SEE(208)는 IC(200)의 보안 동작 모드이다. 예를 들어, SEE(208)는 IC(200)의 비보안 동작 모드에서 실행되는 다른 애플리케이션들에 이용가능하지 않은 특정 하드웨어 모듈들 및 회로들, 이를테면, 제어 로직, 버스들 및 메모리 회로들을 포함하고, 이들에 액세스할 수 있다. SEE(208)는 다른 애플리케이션들(예를 들어, 사용자 애플리케이션들, HLOS, 및 심지어 일부 또는 모든 타입들의 부트 로더들)이 보안 휘발성 메모리 회로(212)에 액세스(예를 들어, 판독 및/또는 기록)할 수 없도록 자신의 보안 휘발성 메모리 회로(212)에 대한 완전한 제어 및 액세스를 가질 수 있다.

[0033] [0039] 그 다음, SEE(208)(예를 들어, 자기 자신의 제어 로직을 사용함)는 자신의 보안 휘발성 메모리 회로(212)에 저장되는 비밀 데이터에 기초하여 비밀 키를 추출(예를 들어, 비밀 키를 생성)할 수 있다. SEE(208)는 이것을 달성하기 위해서 암호 보안 알고리즘을 사용한다. 사용되는 알고리즘은 임의의 하나의 특정 타입의 알고리즘 또는 알고리즘들군에 제한되는 것은 아니다. 일부 비-제한적 예들은 블록 코드 알고리즘들, 확산 코드 알고리즘들 및/또는 반복 코드 알고리즘들을 포함한다. 하나의 예에서, 비밀 데이터와 더불어, 보조 데이터는 비밀 키를 추출하기 위해서 알고리즘에 의해 사용될 수 있다. 보조 데이터는 비보안 애플리케이션들에 의해 액세스가능한 비보안 메모리에 저장될 수 있다. 즉, 보조 데이터가 보안적으로 저장되는 어떠한 요건도 존재하지 않는데, 그 이유는 그것의 노출이 자체적으로 제 1 휘발성 메모리 회로(206)의 비밀 키 및/또는 초기 로직 상태 값들의 보안을 위협하지 않기 때문이다.

[0034] [0040] 휘발성 메모리(예를 들어, SRAM) 기반 PUF(210)는 파워 온 시 실질적으로 동일한 초기 로직 상태 값들을 제공하기 때문에, SEE의 암호 알고리즘은 항상 동일한 비밀 키를 추출할 수 있다. 암호 알고리즘은 초기 로직 상태 값들 중 일부가 상이한 파워 온 사이클들 사이에서 상이한 경우에도 에러 정정 기법들을 사용하여 동일한 비밀 키를 추출할 수 있다. PUF(210)의 초기 로직 상태 값들은 동일하게 제조되는 경우에도 상이한 IC들(200)에 걸쳐 상이하기 때문에, 추출되는 비밀 키는 특정 IC(200)에 고유하다.

[0035] [0041] SEE(208)는 도 2에 도시되는 보안 휘발성 메모리 회로(212)와 같은 보안 휘발성 메모리에 추출된 비밀 키를 저장하고, 따라서, 비보안 애플리케이션들(예를 들어, HLOS, 사용자 애플리케이션들 및/또는 일부 2차 부트 로더들 등)(204)은 SEE(208)에 의해 저장 및 보안되는 비밀 키에 액세스할 수 없다. 대신에, 비보안 애플리케이션들(204)은 비밀 키에 기초하여 암호 데이터 및/또는 공개 데이터(예를 들어, 공개적으로 나타낼 수 있는 데이터)가 제공되도록 SEE(208)에 요청할 수 있다. 예를 들어, SEE(208)는 비밀 키에 기초하여 하나 또는 그

초과의 2차 키들 또는 키-페어들과 같은(그러나, 이들에 제한되는 것은 아님) 암호 데이터를 생성하고, 그 2차 키들을 비보안 애플리케이션들(204)에 제공할 수 있다. SEE는 또한, 비밀 키에 기초하여 디바이스 시리얼 번호와 같은(그러나, 이에 제한되는 것은 아님) 공개 데이터를 생성하고, 그 공개 데이터를 비보안 애플리케이션들(204)에 제공할 수 있다. 암호 데이터 및 공개 데이터 둘 다는 본원에서 "SEE 출력 데이터"로 지칭될 수 있다.

[0036] [0042] 더욱이, 비밀 키는 단지 보안 휘발성 메모리(212)에 저장되기 때문에, 비밀 키는 IC(200)가 파워 오프될 때 손실된다. 그것은 위에서 설명된 바와 같은 PUF(210)의 초기 로직 상태 값들에 기초하여 파워 온 시 다시 재추출되어야 한다. IC(200) 및 검사 메모리 회로들을 물리적으로 개방함으로써 비밀 키로의 허가되지 않은 액세스를 얻으려고 시도하는 비도덕적(nefarious) 당사자는 그 키가 비-휘발성 메모리에 저장되지 않기 때문에 그 키를 획득할 수 없을 것이다.

[0037] [0043] 하나의 양상에 따라, IC(200) 및/또는 휘발성 메모리 회로(206)는 리셋(즉, 파워 오프 및 파워 온, 및/또는 자신의 초기 상태로 리턴) 시 보안 부트 흐름이 즉시 실행되도록(즉, IC(200)가 또한 리셋되도록) 설계된다. 하나의 양상에 따라, RPM 회로(201)는 휘발성 메모리 회로(206)의 리셋을 단독으로 제어할 수 있다. 이로써, 비보안 애플리케이션(204)은 PUF(210) 및/또는 휘발성 메모리 회로(206)를 리셋할 수 없으며, PUF(210)의 초기 로직 상태 값들로의 액세스를 얻을 수 없다. IC(200)의 리셋은 실행 중인 비보안 애플리케이션(204)을 종료시키고, 보안 부트 흐름으로 하여금 다시 시작하게 할 것이다.

[0038] [0044] 하나의 양상에 따라, PUF(210)를 구성하는 특정 휘발성 메모리 회로 셀들은 다양한 방식들로 선택될 수 있다. 하나의 예에 따라, PUF(210)의 메모리 셀들은 신뢰성(즉, 파워 온 시 일관적 로직 상태 값들을 생성할 증가되는 확률)을 위해서 선택되는 메모리 회로 셀들의 인접한 블록일 수 있다. 또 다른 예에 따라, PUF(210)의 메모리 셀들은 서로에 대해 인접하지 않고, 심지어 휘발성 메모리 회로(206)의 다양한 사이트들로부터 랜덤하게 선택될 수 있다. 그러나, 일단 PUF(210)를 구성하는 특정 휘발성 메모리 회로 셀들이 선택되면, 동일한 특정 휘발성 메모리 회로 셀들은 PUF(210)의 기반이 되도록 파워 온될 때마다 다시 선택된다.

[0039] [0045] 휘발성 메모리 회로(206) 및 보안 휘발성 메모리 회로(212)가 도 2의 독립적 회로 블록들로서 도시되지만, 이들은 하나의 양상에 따라 하나의 물리적 휘발성 메모리 회로의 일부일 수 있다. 예를 들어, 보안 휘발성 메모리 회로(212)는 SEE(208)에 의해 배분 및 보안되는 휘발성 메모리 회로(206)의 부분일 수 있다. 그러나, 또 다른 양상에 따라, 2개의 메모리 회로들(206, 212)은 둘다 동일한 IC(200) 상에 로케이팅되는 상이한 메모리 회로들일 수 있다.

[0040] [0046] 도 3은 본 개시 내용의 하나의 양상에 따른 휘발성 메모리 회로(206)의 개략 블록도를 예시한다. 휘발성 메모리 회로(206)는 복수의 휘발성 메모리 회로 셀들을 각각 포함하는 복수의 메모리 모듈들/회로들(210, 302, 304, 306)을 포함할 수 있다. 하나의 예에 따라, 휘발성 메모리 모듈들/회로들(206, 302, 304, 306)은 복수의 SRAM 회로 셀들을 각각 포함하는 SRAM 모듈들/회로들이다. 휘발성 메모리 회로(206)는 PUF 메모리 회로(210)(본원에서 "제 1 휘발성 메모리 회로"로 또한 지칭됨)를 포함한다. 메모리 회로들(210, 302, 304, 306) 모두는 일반적 데이터 및 코드(예를 들어, 사용자 애플리케이션들, 2차 부트 로더 코드 및/또는 HLOS와 관련된 저장 코드)를 저장하는데 사용될 수 있다. 그러나, 하나의 양상에 따라, PUF 메모리 회로(210)의 초기 로직 상태 값들은 메모리 회로(210)가 일반적 데이터 저장을 위해서 사용되기 전에 먼저 클리어되어야 한다. 도 6 및 도 7에 대해 아래에서 더 상세하게 설명될 바와 같이, PUF 메모리 회로(210)의 초기 로직 상태 값들 및/또는 이러한 초기 로직 상태 값들로부터 유추되는 비밀 데이터는 PUF 메모리 회로(210)가 클리어되기 전에 제 2 휘발성 메모리 회로(302)(본원에서 "예비 휘발성 메모리 회로"로 또한 지칭될 수 있음)에 먼저 저장될 수 있다.

[0041] [0047] 도 4는 본 개시 내용의 하나의 양상에 따른 SEE(208)의 개략 블록도를 예시한다. SEE(208)는 보안 휘발성 메모리 회로(212), 제어 회로(402), 및 보안 휘발성 메모리 회로(212) 및 제어 회로(402)와 같은 SEE(208)의 컴포넌트들 사이의 통신을 허용하는 보안 버스 라인(404)을 포함할 수 있다. 제어 회로(402)는 사용자 애플리케이션들, HLOS 및/또는 일부 2차 부트 로더들과 같은 비보안 애플리케이션들보다는, 단지 SEE(208)에 의해 액세스 및 활용될 수 있는 제어 로직이다. 제어 회로(402)는 데이터가 어떻게 보안 휘발성 메모리 회로(212)에 저장 및 카피되고, 보안 휘발성 메모리 회로(212)로부터 판독되는지를 제어할 수 있다. 제어 회로(402)는 또한, PUF(210)(도 2 참조)의 초기 로직 상태 값들로부터 유추되는 비밀 데이터 및 일부 경우들에서 추가 보조 데이터에 기초하여 비밀 키를 추출하는 본원에서 논의되는 암호 알고리즘들을 실행시킬 수 있다. 제어 회로(402)는 비밀 키에 기초하여 추가 2차 키들 및/또는 공개 데이터를 추가로 생성할 수 있다. 따라서, SEE 제어 회로(402)는 비밀 데이터에 기초하여 비밀 키를 추출하기 위해서 SEE에서 암호 알고리즘을 실행시키기 위한 수단의 하나의 예를 표현한다.

[0042] [0048] 보안 휘발성 메모리 회로(212)는 복수의 메모리 셀들을 각각 포함하는 하나 또는 그 초과의 보안 휘발성 메모리 회로들을 포함한다. 보안 휘발성 메모리 회로(212)는 eDRAM, SRAM 등과 같은(그러나, 이들에 제한되는 것은 아님) 임의의 타입의 휘발성 메모리일 수 있다. 보안 휘발성 메모리 회로(212)는 비밀 데이터 및 또한 비밀 데이터에 부분적으로 기초하여 제어 로직(402)에 의해 추출되는 비밀 키를 저장한다. SEE(208)는 다른 애플리케이션들(예를 들어, 비보안 애플리케이션)이 보안 휘발성 메모리 회로(212)에 액세스할 수 없도록 보안 휘발성 메모리 회로(212)에 대한 완전한 제어를 수행한다. 예를 들어, SEE(208)는 보안 휘발성 메모리 회로(212)를 IC(200)의 다른 비보안 회로에 커플링시키는 임의의 버스(408) 라인들을 물리적으로 록 다운(lock down)시킬 수 있다(디스에이블 버스 로직(406)으로서 도시됨).

[0043] [0049] 도 5는 본 개시 내용의 하나의 양상에 따른 보안 부트 흐름(500) 계층을 예시한다. IC(200)(예를 들어, 그것의 프로세싱 회로(203))에 의해 실행될 수 있는 보안 부트 흐름(500)은 부분적으로 보안 부트 로더(501)에 의해 그리고 부분적으로 비보안 애플리케이션 로더(503)에 의해 포함될 수 있다. 보안 부트 로더(501)는 PBL(primary boot loader)(502), SBL_1(first secondary boot loader)(504) 및 SBL_2(second secondary boot loader)(506)를 포함할 수 있다. 보안 부트 로더(501)에 의해 실행되는 코드는 어떠한 허가되지 않은 사용자 코드(예를 들어, HLOS, 사용자 애플리케이션들 등)도 부트 업 프로세스의 이 부분 동안 실행 및/또는 주입되지 않을 수 있으므로 "보안적"인 것으로 고려된다. 따라서, PUF(210)(도 2 참조)의 초기 로직 상태 값들과 관련된 정보, 이러한 초기 로직 상태 값들로부터 유추되는 비밀 데이터 및/또는 비밀 데이터에 기초하여 추출되는 비밀 키는 보안 부트 흐름(500)의 이 부분 동안 허가되지 않은 애플리케이션들에 절충/누설될 위험이 적다.

[0044] [0050] 비보안 애플리케이션 로더(503)는 SBL_3(third secondary boot loader)(508), 애플리케이션 2차 부트 로더(510), HLOS(512) 및 사용자 애플리케이션들(514)을 포함할 수 있다. 비보안 애플리케이션 로더(503)는 허가되지 않은 사용자 코드가 이 로더들(508, 510, 512, 514) 중 하나 또는 그 초과의 로더들의 실행 및/또는 인증 동안 실행 및/또는 주입될 수 있으므로 "비보안적"인 것으로 고려된다.

[0045] [0051] 도 2 및 도 5를 참조하면, IC(200)의 파워 온 시, 보안 부트 흐름(500)은 IC(200)의 다양한 회로들 및 모듈들의 초기화를 포함한, IC(200)의 가장 초기 그리고 기본적 태스크들 중 일부를 수행하는 1차 부트 로더(502)의 실행으로 시작된다. PBL(502)은 하드-와이어링(예를 들어, ROM에 저장)될 수 있으며, 따라서, 그것은 사실상 교번될 수 없기 때문에 매우 보안적이다. PBL(502)은 또한, SBL_1(504)이 실행되기 전에 SBL_1(504)을 로딩 및 인증한다. SBL_1(504)의 인증 이후, SBL_1(504)은 실행되며, 그 중에서도, 휘발성 메모리 회로(206)의 초기 로직 상태 값들에 기초하여 비밀 데이터를 유추하고, IC(200) 내의 다른 메모리 회로들에 비밀 데이터를 저장할 수 있다. SBL_1(504)은 또한: RPM 회로(201)를 초기화하고; IC(200) 시스템 클럭을 구성시키며 리셋을 릴리스(release)하고; 그리고 SBL_2(506)가 실행되기 전에 SBL_2(506)를 로딩 및 인증할 수 있다.

[0046] [0052] SBL_2(506)가 인증된 이후, SBL_2(506)는 실행되며, 그 중에서도, 비보안 메모리 회로로부터 보안 휘발성 메모리 회로(212)로 비밀 데이터를 카피할 수 있다. SBL_2(506)는 또한: IC(200)의 하나 또는 그 초과의 프로세싱 회로들(예를 들어, 프로세싱 회로(203))을 초기화하고; IC(200) 외부의 메모리 회로들(예를 들어, 외부의 DRAM 및/또는 SRAM)을 구성시키고; SEE(208), 다른 펌웨어 및/또는 SBL_3(508)을 로딩 및 인증할 수 있다. SBL_3(508)의 인증 이후, SBL_3(508)은 실행되며, 그 중에서도, 소프트웨어 플래싱을 위해서 저장 모드를 체크할 수 있다. SBL_3(508)은 또한, HLOS(512) 및/또는 애플리케이션 2차 부트 로더(510)를 로딩 및 인증할 수 있다. 유사한 방식으로, 후속하는 부트 업 프로세스들, 이를테면, 애플리케이션 2차 부트 로더(510), HLOS(512) 및 사용자 애플리케이션들(514)은 연속적 순서로 로딩, 인증 및 실행된다. 이 프로세스들(502, 504, 506, 508, 510, 512)이 로딩 및 실행되는 순서는 도 5에 도시되는 것과 다를 수 있다. 더욱이, 2차 부트 로더들의 수 및 타입, 및 도 5에 도시되는 다른 애플리케이션 코드는 단지 설명적/예시적이다. 예를 들어, 본 개시 내용의 다른 양상들에서, 더 많거나 또는 더 적은 2차 부트 로더들은 보안 부트 흐름(500)을 포함할 수 있다.

[0047] [0053] 도 6은 본 개시 내용의 하나의 양상에 따른, 비밀 키를 추출하여 저장하는 본원에서 설명되는 보안 부트 흐름을 특징화하는 IC(600)를 예시한다. IC(600)는 RPM 회로(201), 프로세싱 회로(예를 들어, 애플리케이션 프로세서)(203), 보안 부트 로더(501), 비보안 애플리케이션 부트 로더(503), 휘발성 메모리 회로(206), SEE(208) 및/또는 비-휘발성 메모리 회로(604)를 포함할 수 있다. 보안 부트 로더(501)는 PBL(502), SBL_1(504) 및/또는 SBL_2를 포함할 수 있다. 비보안 애플리케이션 부트 로더(503)는 SBL_2(506)(도 5 참조) 이후 실행되는 보안 부

트 흐름(500)의 부분에 대한 부트 로더들을 포함할 수 있다. 예를 들어, 비보안 애플리케이션 부트 로더(503)는 SBL_3(508), 애플리케이션 2차 부트 로더(510), HLOS 코드(512) 및/또는 사용자 애플리케이션들(514)을 포함할 수 있다. 휘발성 메모리 회로(206)는 제 1 휘발성 메모리 회로(210)(즉, PUF) 및 제 2/예비 휘발성 메모리 회로(302)를 포함한다. SEE(208)는 SEE 제어 회로(402) 및 보안 휘발성 메모리 회로(212)를 포함한다. 보안 휘발성 메모리 회로(212)는 PUF의 초기 로직 상태 값들로부터 유추되는 비밀 데이터를 저장하도록 구성되는 제 1 보안 휘발성 메모리 회로(608) 및 비밀 키를 저장하도록 구성되는 제 2 보안 휘발성 메모리 회로(610)를 포함한다.

[0048] [0054] 비-휘발성 메모리 회로(604)는 보조 데이터(606)를 포함한다. 하나의 예에 따라, 비-휘발성 메모리 회로(604)는 IC(600)의 일부(즉, 그것은 "온-칩"임)이다. 또 다른 예에 따라, 비-휘발성 메모리 회로(604)는 IC(600)의 일부가 아니며, IC(600)과 통신하는 별개의 회로(즉, 그것은 "오프-칩"임)이다. 보조 데이터(606) 전부 또는 그 중 일부는 그것이 비보안 애플리케이션들에 의해 액세스될 수 있으므로 비보안적일 수 있다. 제 1 보안 휘발성 메모리 회로(608)는 보안 휘발성 메모리 회로에 비밀 데이터를 저장하기 위한 수단의 하나의 예를 표현하고, 제 2 보안 휘발성 메모리 회로(610)는 보안 휘발성 메모리 회로에 비밀 키를 저장하기 위한 수단의 하나의 예를 표현한다.

[0049] [0055] 도 7a 및 도 7b를 포함하는 도 7은 하나의 양상에 따른, 집적 회로(600)로 하여금 비밀 키를 추출하여 저장하게 하는 보안 부트 흐름을 도시하는 흐름도(700)를 예시한다. 도 6 및 도 7을 참조하면, IC(600)의 파워 온 시, 제 1 휘발성 메모리 회로(210)(즉, PUF에 대해 사용되는 메모리의 부분)를 포함하는 휘발성 메모리 회로(206)에 파워가 공급된다. 도 2에 대해 위에서 설명된 바와 같이, 휘발성 메모리 회로(206)는 SRAM과 같은 휘발성 메모리 타입을 가지며, 휘발성 메모리 회로(206)의 메모리 회로 셀들은 전형적으로, 각각의 셀에 고유한 제조 세부사항들에 기인하여 파워 온 시 선호되는 로직 상태로 초기에 각각 놓일 것이다. 초기 로직 값들은, 스타트-업(즉, 파워 온) 시 대다수의 셀들이 매번 동일한 값으로 놓일 것이도록 실질적으로 반복가능하다. 따라서, 파워 온 시 PUF에 대해 사용되는 제 1 휘발성 메모리 회로(210)를 포함하는 휘발성 메모리 회로(206)는 초기 로직 상태 값들로 놓인다(702).

[0050] [0056] 다음으로, 제 1 2차 부트 로더(SBL_1)(504)는 휘발성 메모리 회로(206)의 메모리 회로 셀들을 로케이팅하고 - 휘발성 메모리 회로(206)의 초기 로직 상태 값들이 사용될 수 있을 것임 (즉, 메모리의 부분은 제 1 휘발성 메모리 회로(210)를 지정함) - , 그러한 초기 로직 상태 값들에 기초하여 비밀 데이터를 유추한다(704). 위에서 설명된 바와 같이, 비밀 데이터는 초기 로직 상태 값들과 동일할 수 있거나 또는 비밀 데이터는 초기 로직 상태 값들의 일부 함수에 기초하여 유추될 수 있다. 비밀 데이터가 유추된 이후, SBL_1(504)은 휘발성 메모리 회로(706)의 제 2(즉, 예비) 메모리 부분(302)에 비밀 데이터를 저장한다. 그 다음, SBL_1(504)은 초기 로직 상태 값들의 어떠한 흔적도 후속하는 프로세스들/애플리케이션들(예를 들어, 비보안 애플리케이션들)에 의해 그러한 메모리 어드레스 위치들에서 발견되지 않을 수 있도록 제 1 휘발성 메모리 회로(210)의 초기 로직 상태 값들을 클리어한다. 일단 클리어되면, 제 1 휘발성 메모리 회로(210)는 일반적 데이터 저장에 이용가능하다(즉, 임의의 후속하는 프로세스/애플리케이션은 그 제 1 휘발성 메모리 회로(210)를 사용할 수 있음)(708).

[0051] [0057] 그 다음, SBL_2(second secondary boot loader)(506)는 제 2 메모리 부분(302)에 저장되는 비밀 데이터를 SEE(208)의 보안 휘발성 메모리 회로(212)에 카피/전달한다. 예를 들어, 보안 데이터는 may be stored at the 제 1 보안 휘발성 메모리 회로(608)에 저장될 수 있다. 그 다음, SBL_2(506)는 휘발성 메모리 회로(206)에서의 비밀 데이터의 임의의 트레이스를 제거하기 위해서 휘발성 메모리 회로(206)의 제 2 메모리 부분(302)을 클리어하고 그리고/또는 전체 휘발성 메모리 회로(206)를 클리어한다. 일단 클리어되면, 예비 메모리 부분(302)은 일반적 데이터 저장에 이용가능하다(즉, 임의의 후속하는 프로세스/애플리케이션은 그 예비 메모리 부분(302)을 사용할 수 있음)(712).

[0052] [0058] 추가로, SEE(208)는 그 다음, 비밀 데이터에 기초하여 비밀 키를 추출한다. 예를 들어, SEE(208)에서의 제어 로직 회로(402)는 제 1 보안 휘발성 메모리 회로(608)에 저장된 비밀 데이터 및 비-휘발성 메모리 회로(604)에 저장된 보조 데이터(606)를 획득한다. 이 데이터를 획득한 이후, 제어 회로(402)는 비밀 키를 추출하기 위해서 입력들로서 보조 데이터(606) 및 비밀 데이터를 사용하여 암호 알고리즘(예를 들어, 블록 코드 알고리즘, 확산 코드 알고리즘, 반복 코드 알고리즘 등 중 적어도 하나)을 실행시킨다. 암호 알고리즘은, 하나의 부트로부터 다음의 부트로의 비밀 데이터 및/또는 초기 로직 상태 값들 사이의 일부 차이들에도 불구하고, 동일한 비밀 키를 추출하기 위한 에러 정정 기법들을 포함할 수 있다. 비밀 키는 또한, 보안 휘발성 메모리(212)

(예를 들어, 제 2 보안 휘발성 메모리 회로(610))에 저장된다(714).

[0053] [0059] 비밀 키는 보안 휘발성 메모리 회로(212)에 SEE(208)의 제어 내에서 보안적으로 저장되기 때문에, 비밀 키는 다른 비보안 애플리케이션들에 의해 액세스될 수 없다. 이러한 비보안 애플리케이션들은 비밀 키에 기초하여 SEE 출력 데이터(예를 들어, 위에서 설명된 바와 같이, 암호 데이터 및/또는 공개 데이터를 포함함)에 대한 요청들을 SEE(208)에 전송할 수 있다(716). SEE(208)에서의 제어 로직 회로(402)는 그 다음, 비밀 키에 기초하여 SEE 출력 데이터를 생성하고, SEE 출력 데이터를 요청하는 비보안 애플리케이션에 제공할 수 있다(718).

[0054] [0060] 비밀 키는 단지 보안 휘발성 메모리(212)에 저장되기 때문에, 비밀 키는 IC(600)가 파워 오프될 때 손실된다. 그것은 위에서 설명된 바와 같은 PUF(210)의 초기 로직 상태 값들에 기초하여 파워 온 시 보안 부트 흐름(700)을 통해 다시 재추출되어야 한다. IC(600) 및 검사 메모리 회로들을 물리적으로 개방함으로써 비밀 키로의 허가되지 않은 액세스를 얻으려고 시도하는 비도덕적 당사자는 그 키가 비-휘발성 메모리에 저장되지 않기 때문에 그 키를 획득할 수 없을 것이다.

[0055] [0061] 하나의 양상에 따라, IC(600) 및/또는 휘발성 메모리 회로(206)는 리셋 시 보안 부트 흐름(700)이 즉시 실행되도록(즉, IC(600)가 또한 리셋되도록) 설계된다. 하나의 양상에 따라, RPM 회로(201)는 휘발성 메모리 회로(206)의 리셋을 단독으로 제어할 수 있다. 이로써, 비보안 애플리케이션은 PUF(210) 및/또는 휘발성 메모리 회로(206)를 리셋할 수 없으며, PUF(210)의 초기 로직 상태 값들로의 액세스를 얻을 수 없다. IC(600)의 리셋은 실행 중인 비보안 애플리케이션을 종료시키고, 보안 부트 흐름(700)으로 하여금 다시 시작하게 할 것이다.

[0056] [0062] 하나의 양상에 따라, PUF(210)를 구성하는 특정 휘발성 메모리 회로 셀들은 다양한 방식들로 선택될 수 있다. 하나의 예에 따라, PUF(210)의 메모리 셀들은 신뢰성(즉, 파워 온 시 일관적 로직 상태 값들을 생성할 증가되는 확률)을 위해서 선택되는 메모리 회로 셀들의 인접한 블록일 수 있다. 또 다른 예에 따라, PUF(210)의 메모리 셀들은 서로에 대해 인접하지 않고, 심지어 휘발성 메모리 회로(206)의 다양한 사이트들로부터 랜덤하게 선택될 수 있다. 그러나, 일단 PUF(210)를 구성하는 특정 휘발성 메모리 회로 셀들이 선택되면, 동일한 특정 휘발성 메모리 회로 셀들은 PUF(210)의 기반이 되도록 파워 온될 때마다 다시 선택된다.

[0057] [0063] 도 8은 본 개시 내용의 하나의 양상에 따른, 집적 회로에서 동작가능한 방법(800)을 예시한다. 먼저, 제 1 휘발성 메모리 회로는 복수의 초기 로직 상태 값들을 생성하기 위해서 파워 온된다 – 여기서, 제 1 휘발성 메모리 회로는 집적 회로 상에 있음 – (802). 다음으로, 비밀 데이터는 복수의 초기 로직 상태 값들에 기초하여 유추된다(804). 그 다음, 비밀 데이터는 보안 휘발성 메모리 회로에 저장된다 – 여기서, 보안 휘발성 메모리 회로는 SEE(secure execution environment)에 의해 보안된다(806). 다음으로, 복수의 초기 로직 상태 값들은 제 1 휘발성 메모리 회로에서 클리어된다(808). 그 다음, 암호 알고리즘은 비밀 데이터에 기초하여 비밀 키를 추출하기 위해서 SEE에서 실행된다(810). 비밀 키는 또한, 보안 휘발성 메모리 회로(812)에 저장된다. 하나의 양상에 따라, 비밀 키는 복수의 초기 로직 상태 값들이 제 1 휘발성 메모리 회로에서 클리어(단계(808))되기 전에 추출 및 저장될 수 있다(즉, 단계들(810, 812)).

[0058] [0064] 도 9는 본 개시 내용의 하나의 양상에 따른, IC들(200, 600)의 프로세싱 회로(203)의 개략 블록도를 예시한다. 프로세싱 회로(203)는 비밀 데이터 유추 회로(902), 클리어링 회로(904) 및/또는 암호 알고리즘 회로(906)를 포함할 수 있다.

[0059] [0065] 도 2, 도 6, 도 8 및 도 9를 참조하면, 비밀 데이터 유추 회로(902)는 복수의 초기 로직 상태 값들에 기초하여 비밀 데이터를 유추하기 위한 수단의 하나의 예이다. 클리어링 회로(904)는 제 1 휘발성 메모리 회로(206)에서 복수의 초기 로직 상태 값들을 클리어하기 위한 수단의 하나의 예이다. 암호 알고리즘 회로(906)는 비밀 데이터에 기초하여 비밀 키를 추출하기 위해서 SEE(208)에서 암호 알고리즘을 실행하기 위한 수단의 하나의 예이다.

[0060] [0066] 도 2, 도 3, 도 4, 도 5, 도 6, 도 7a, 도 7b, 도 8 및 도 9에 예시되는 컴포넌트들, 단계들, 특징들 및/또는 기능들 중 하나 또는 그 초과의 것들은, 단일 컴포넌트, 단계, 특징 또는 기능으로 재배열 및/또는 결합되거나, 또는 몇몇 컴포넌트들, 단계들 또는 기능들로 구현될 수 있다. 추가 엘리먼트들, 컴포넌트들, 단계들 및/또는 기능들은 또한, 본 발명으로부터 벗어나지 않고 추가될 수 있다. 도 2, 도 3, 도 4, 도 6 및/또는 도 9에 예시되는 장치, 디바이스들 및/또는 컴포넌트들은 도 5, 도 7a, 도 7b, 및/또는 도 8에서 설명되는 방법들, 특징들 또는 단계들 중 하나 또는 그 초과의 것을 수행하도록 구성될 수 있다. 또한, 본원에서 설명되는 알고리즘들은 또한 효율적으로, 소프트웨어로 구현되고 그리고/또는 하드웨어에 임베딩될 수 있다.

[0061] [0067] 더욱이, 본 개시 내용의 하나의 양상에서, 도 2, 도 6 및/또는 도 9에 예시되는 프로세싱 회로(203)는

도 5, 도 7a, 도 7b 및/또는 도 8에 설명되는 알고리즘들, 방법들 및/또는 단계들을 수행하기 위해서 특정적으로 설계 및/또는 하드-와이어링되는 특수화된 프로세서(예를 들어, 주문형 집적 회로(예를 들어, ASIC))일 수 있다. 따라서, 이러한 특수화된 프로세서(예를 들어, ASIC)는 도 5, 도 7a, 도 7b 및/또는 도 8에서 설명되는 알고리즘들, 방법들 및/또는 단계들을 실행시키기 위한 수단의 하나의 예일 수 있다.

[0062] [0068] 또한, 본 개시 내용의 양상들은 순서도(flowchart), 흐름도, 구조도 또는 블록도로서 도시되는 프로세스로서 설명될 수 있다는 점이 주목된다. 순서도는 순차적 프로세스로서 동작들을 설명할 수 있지만, 동작들 중 많은 동작들이 동시에 또는 동시적으로 수행될 수 있다. 또한, 동작들의 순서는 재배열될 수 있다. 프로세스는 그것의 동작들이 완료될 때 종료된다. 프로세스는 방법, 함수, 프로시저, 서브루틴, 서브프로그램 등에 대응할 수 있다. 프로세스가 함수에 대응하는 경우, 그것의 종료는 호출 함수 또는 메인 함수으로의 함수의 리턴에 대응한다.

[0063] [0069] 더욱이, 저장 매체는 ROM(read-only memory), RAM(random access memory), 자기 디스크 저장 매체들, 광학 저장 매체들, 플래시 메모리 디바이스들, 및/또는 정보를 저장하기 위한 다른 머신 판독가능한 매체들 및 프로세서 판독가능한 매체들 및/또는 컴퓨터 판독가능한 매체들을 포함하는, 데이터를 저장하기 위한 하나 또는 그 초과의 디바이스들을 표현할 수 있다. "머신 판독가능한 매체", "컴퓨터 판독가능한 매체" 및/또는 "프로세서 판독가능한 매체"라는 용어들은 휴대용 또는 고정용 저장 디바이스들, 광학 저장 디바이스들, 및 명령(들) 및/또는 데이터를 저장 또는 포함할 수 있는 다양한 다른 매체들과 같은 비-일시적 매체들을 포함할 수 있지만, 이들에 제한되는 것은 아니다. 따라서, 본원에서 설명되는 다양한 방법들은 전체적으로 또는 부분적으로, "머신 판독가능한 매체", "컴퓨터 판독가능한 매체" 및/또는 "프로세서 판독가능한 매체"에 저장될 수 있는 명령들 및/또는 데이터에 의해 구현되고, 하나 또는 그 초과의 프로세서들, 머신들 및/또는 디바이스들에 의해 실행될 수 있다.

[0064] [0070] 게다가, 본 개시 내용의 양상들은 하드웨어, 소프트웨어, 펌웨어, 미들웨어, 마이크로코드 또는 이들의 임의의 결합에 의해 구현될 수 있다. 소프트웨어, 펌웨어, 미들웨어 또는 마이크로코드로 구현되는 경우, 필요한 태스크들을 수행하기 위한 프로그램 코드 또는 코드 세그먼트들은 머신 판독가능한 매체, 이를테면, 저장 매체 또는 다른 저장소(들)에 저장될 수 있다. 프로세서는 필요한 태스크들을 수행할 수 있다. 코드 세그먼트는 프로시저, 함수, 서브프로그램, 프로그램, 루틴, 서브루틴, 모듈, 소프트웨어 패키지, 클래스, 또는 명령들, 데이터 구조들 또는 프로그램 명령문들의 임의의 결합을 표현할 수 있다. 코드 세그먼트는 정보, 데이터, 인자들, 파라미터들 또는 메모리 컨텐츠를 전달 및/또는 수신함으로써 다른 코드 세그먼트 또는 하드웨어 회로에 커플링될 수 있다. 정보, 인자들, 파라미터들, 데이터 등은 메모리 공유, 메시지 전달, 토큰 전달, 네트워크 송신 등을 포함하는 임의의 적합한 수단을 통해 전달, 포워딩 또는 송신될 수 있다.

[0065] [0071] 본원에서 개시되는 예들과 관련하여 설명된 다양한 예시적 로직 블록들, 모듈들, 회로들, 엘리먼트들 및/또는 컴포넌트들이 범용 프로세서, DSP(digital signal processor), ASIC(application specific integrated circuit), FPGA(field programmable gate array) 또는 다른 프로그래머블 로직 컴포넌트, 이산 게이트 또는 트랜지스터 로직, 이산 하드웨어 컴포넌트들, 또는 본원에서 설명되는 기능들을 수행하도록 설계되는 이들의 임의의 결합으로 구현되거나 또는 수행될 수 있다. 범용 프로세서는 마이크로프로세서일 수 있지만, 대안적으로, 프로세서는 임의의 종래의 프로세서, 제어기, 마이크로제어기, 또는 상태 머신일 수 있다. 프로세서는 또한 컴퓨팅 컴포넌트들의 결합, 예를 들어, DSP 및 마이크로프로세서의 결합, 다수의 마이크로프로세서들, DSP 코어와 결합된 하나 또는 그 초과의 마이크로프로세서들, 또는 임의의 다른 이러한 구성으로서 구현될 수 있다.

[0066] [0072] 본원에서 개시되는 예들과 관련하여 설명되는 알고리즘들 또는 방법들은 직접 하드웨어로, 프로세서에 의해 실행되는 소프트웨어 모듈로, 또는 이 둘의 결합으로, 프로세싱 유닛, 프로그래밍 명령들 또는 다른 지시들의 형태로 구현될 수 있으며, 단일 디바이스에 포함되거나 또는 다수의 디바이스들에 걸쳐 분산될 수 있다. 소프트웨어 모듈은 RAM 메모리, 플래시 메모리, ROM 메모리, EPROM 메모리, EEPROM 메모리, 레지스터들, 하드디스크, 이동식(removable) 디스크, CD-ROM, 또는 당해 기술 분야에 공지된 임의의 다른 형태의 저장 매체에 상주할 수 있다. 저장 매체는, 프로세서가 저장 매체로부터 정보를 판독하고, 저장 매체에 정보를 기록할 수 있도록 프로세서에 커플링될 수 있다. 대안적으로, 저장 매체는 프로세서에 통합될 수 있다.

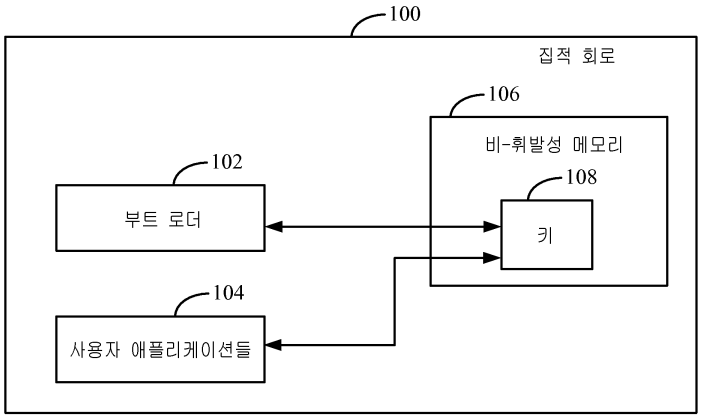
[0067] [0073] 당업자들은, 본원에서 개시되는 양상들과 관련하여 설명된 다양한 예시적 로직 블록들, 모듈들, 회로들 및 알고리즘 단계들이 전자 하드웨어, 컴퓨터 소프트웨어, 또는 이 둘의 결합들로서 구현될 수 있다는 것을 추가로 인식할 것이다. 하드웨어와 소프트웨어의 이러한 상호 호환성을 명확하게 예시하기 위해서, 다양한 예시적 컴포넌트들, 블록들, 모듈들, 회로들 및 단계들이 일반적으로 이들의 기능적 관점에서 위에서 설명되었다.

이러한 기능이 하드웨어로서 구현되는지 또는 소프트웨어로서 구현되는지는 전체 시스템 상에 부과되는 설계 제약들 및 특정 애플리케이션에 의존한다.

[0068] [0074] 본원에서 설명되는 발명의 다양한 특징들은 본 발명으로부터 벗어나지 않으면서 상이한 시스템들로 구현될 수 있다. 본 개시 내용의 위의 양상들은 단지 예들일 뿐이고, 본 발명을 제한하는 것으로 해석되는 것은 아니라는 점이 주목되어야 한다. 본 개시 내용의 양상들의 설명은 청구항들의 범위를 제한하는 것이 아니라 예시하는 것으로 의도된다. 이로써, 본 교시 내용들은 다른 타입들의 장치들에 쉽게 적용될 수 있고, 많은 대안들, 수정들 및 변형들이 당업자들에게 명백할 것이다.

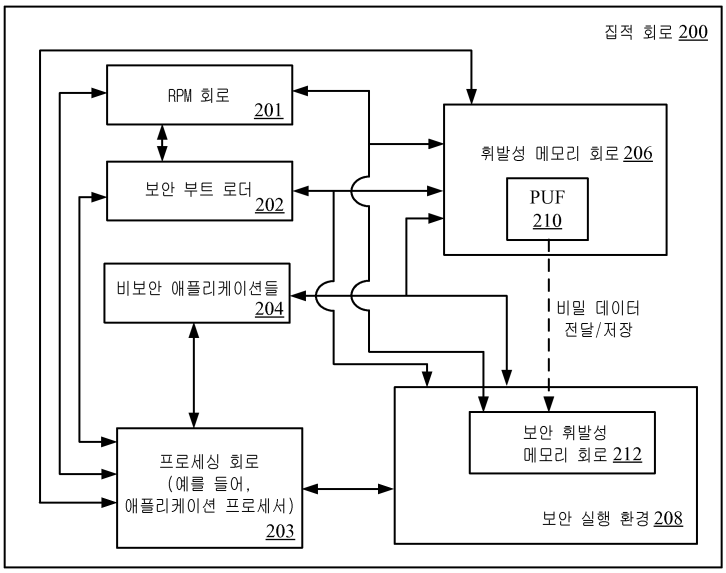
도면

도면1

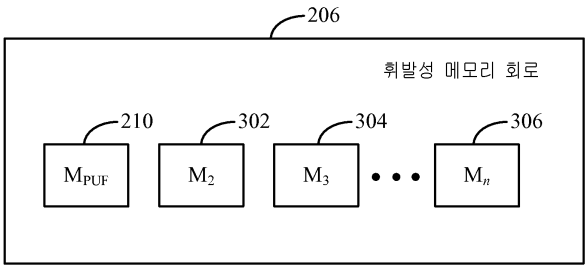


(종래 기술)

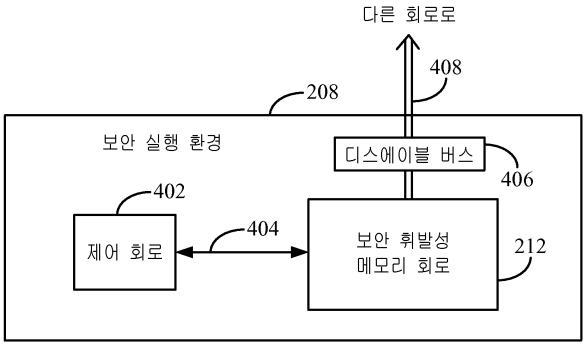
도면2



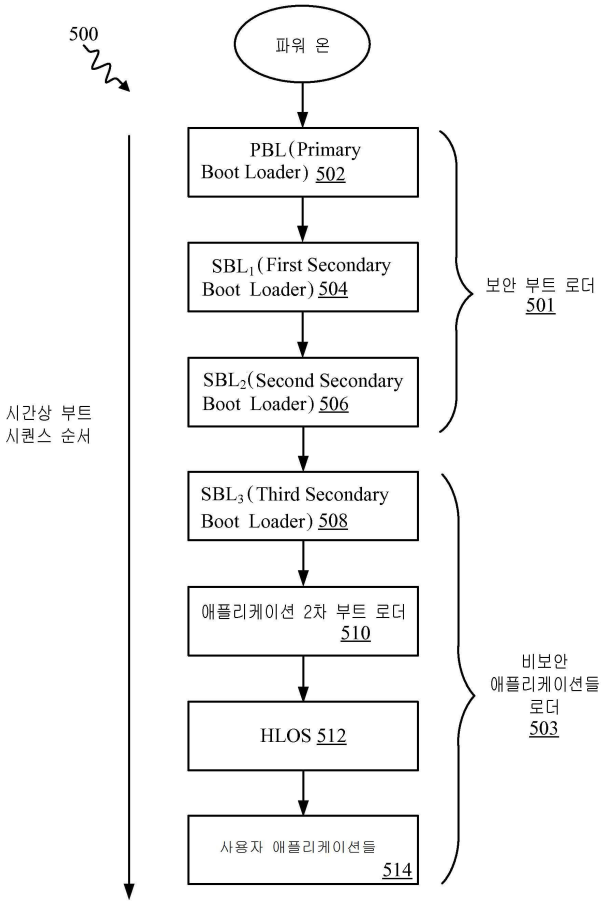
도면3


206
휘발성 메모리 회로
210
302
304
306
M_{PUF}
M_2
M_3
M_n

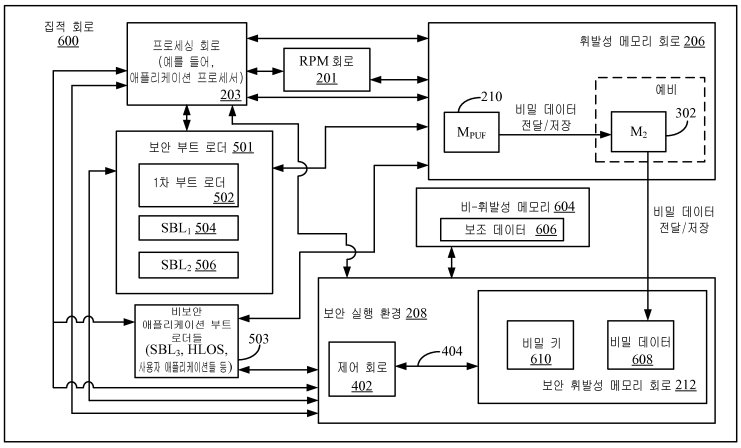
도면4


다른 회로로
408
208
보안 실행 환경
디스에이블 버스
406
402
404
제어 회로
보안 휘발성
메모리 회로
212

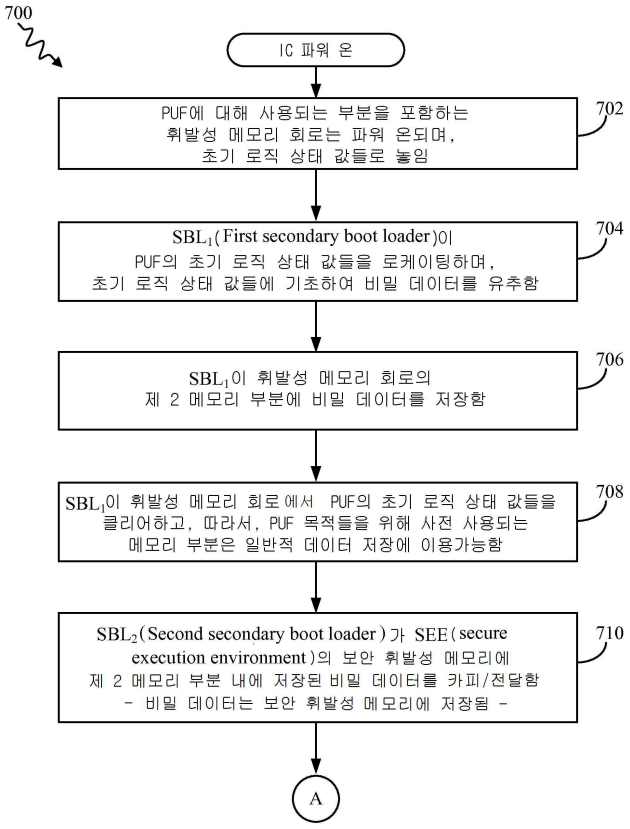
도면5


500
파워 온
PBL (Primary Boot Loader) 502
SBL_1 (First Secondary Boot Loader) 504
SBL_2 (Second Secondary Boot Loader) 506
보안 부트 로더 501
SBL_3 (Third Secondary Boot Loader) 508
애플리케이션 2차 부트 로더 510
HLOS 512
사용자 애플리케이션들 514
비보안 애플리케이션들 로더 503
시간상 부트 시퀀스 순서

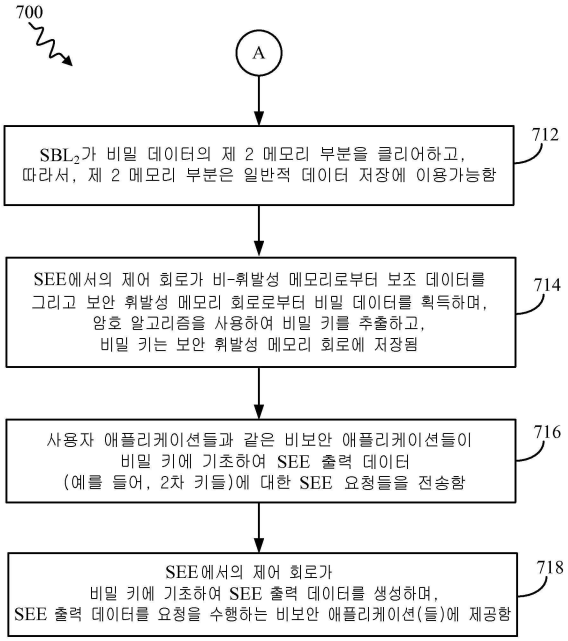
도면6


집적 회로
600
프로세싱 회로
(예를 들어,
애플리케이션 프로세서)
203
RPM 회로
201
휘발성 메모리 회로 206
예비
210
비밀 데이터
전달/저장
302
보안 부트 로더 501
1차 부트 로더
502
SBL1 504
SBL2 506
비-휘발성 메모리 604
보조 데이터 606
비밀 데이터
전달/저장
비보안
애플리케이션 부트
로더들
(SBL3, HLOS,
사용자 애플리케이션들 등)
503
보안 실행 환경 208
제어 회로
402
404
비밀 키
610
비밀 데이터
608
보안 휘발성 메모리 회로 212

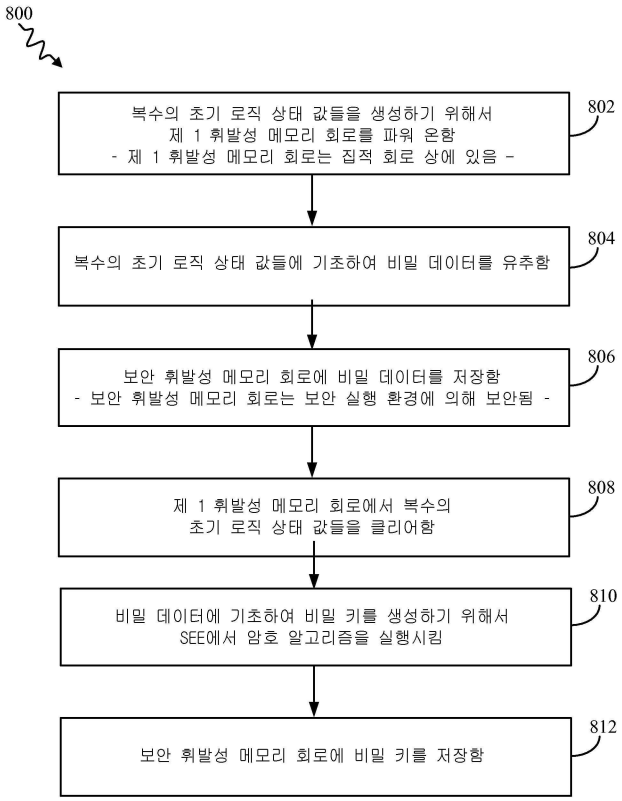
도면7a


700
IC 파워 온
PUF에 대해 사용되는 부분을 포함하는
휘발성 메모리 회로는 파워 온되며,
초기 로직 상태 값들로 놓임
702
SBL1(First secondary boot loader)이
PUF의 초기 로직 상태 값들을 로케이팅하며,
초기 로직 상태 값들에 기초하여 비밀 데이터를 유추함
704
SBL1이 휘발성 메모리 회로의
제 2 메모리 부분에 비밀 데이터를 저장함
706
SBL1이 휘발성 메모리 회로에서 PUF의 초기 로직 상태 값들을
클리어하고, 따라서, PUF 목적들을 위해 사전 사용되는
메모리 부분은 일반적 데이터 저장에 이용가능함
708
SBL2(Second secondary boot loader)가 SEE(secure
execution environment)의 보안 휘발성 메모리에
제 2 메모리 부분 내에 저장된 비밀 데이터를 카피/전달함
- 비밀 데이터는 보안 휘발성 메모리에 저장됨 -
710
A

도면7b


700
A
SBL2가 비밀 데이터의 제 2 메모리 부분을 클리어하고,
따라서, 제 2 메모리 부분은 일반적 데이터 저장에 이용가능함
712
SEE에서의 제어 회로가 비-휘발성 메모리로부터 보조 데이터를
그리고 보안 휘발성 메모리 회로로부터 비밀 데이터를 획득하며,
암호 알고리즘을 사용하여 비밀 키를 추출하고,
비밀 키는 보안 휘발성 메모리 회로에 저장됨
714
사용자 애플리케이션들과 같은 비보안 애플리케이션들이
비밀 키에 기초하여 SEE 출력 데이터
(예를 들어, 2차 키들)에 대한 SEE 요청들을 전송함
716
SEE에서의 제어 회로가
비밀 키에 기초하여 SEE 출력 데이터를 생성하며,
SEE 출력 데이터를 요청을 수행하는 비보안 애플리케이션(들)에 제공함
718

도면8


800
복수의 초기 로직 상태 값들을 생성하기 위해서
제 1 휘발성 메모리 회로를 파워 온함
- 제 1 휘발성 메모리 회로는 집적 회로 상에 있음 -
802
복수의 초기 로직 상태 값들에 기초하여 비밀 데이터를 유추함
804
보안 휘발성 메모리 회로에 비밀 데이터를 저장함
- 보안 휘발성 메모리 회로는 보안 실행 환경에 의해 보안됨 -
806
제 1 휘발성 메모리 회로에서 복수의
초기 로직 상태 값들을 클리어함
808
비밀 데이터에 기초하여 비밀 키를 생성하기 위해서
SEE에서 암호 알고리즘을 실행시킴
810
보안 휘발성 메모리 회로에 비밀 키를 저장함
812

도면9