(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2021년04월12일
(11) 등록번호 10-2239711
(24) 등록일자 2021년04월07일

(51) 국제특허분류(Int. Cl.)
*H04L 9/08* (2006.01) *G06F 21/51* (2013.01)
*G06F 21/57* (2013.01) *G06F 21/79* (2013.01)
*H04L 29/06* (2006.01) *H04L 9/32* (2006.01)
*H04W 12/10* (2021.01) *H04W 12/12* (2021.01)
*H04W 88/02* (2009.01)
(52) CPC특허분류
*H04L 9/0866* (2013.01)
*G06F 21/51* (2013.01)
(21) 출원번호 10-2015-7032856
(22) 출원일자(국제) 2014년04월16일
심사청구일자 2019년04월02일
(85) 번역문제출일자 2015년11월17일
(65) 공개번호 10-2016-0004308
(43) 공개일자 2016년01월12일
(86) 국제출원번호 PCT/US2014/034414
(87) 국제공개번호 WO 2014/176101
국제공개일자 2014년10월30일
(30) 우선권주장
13/868,859 2013년04월23일 미국(US)
(56) 선행기술조사문헌
US07216238 B2*
*(뒷면에 계속)*
전체 청구항 수 : 총 19 항

(73) 특허권자
**퀄컴 인코포레이티드**
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
**아쉬케나지, 아사프**
미국 92121 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(74) 대리인
**특허법인 남앤남**

심사관 : 최재귀

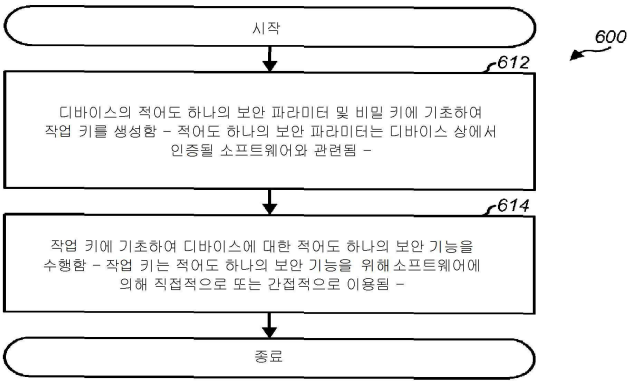
(54) 발명의 명칭 **보안 파라미터들에 기초한 작업 보안 키의 생성**

## (57) 요 약

전자 디바이스의 보안을 개선하기 위한 기법들이 개시된다. 본 개시의 일 양상에서, 디바이스의 보안은, 예를 들어, 키 유도 함수를 갖는 디바이스의 하드웨어 비밀 키 및 적어도 하나의 보안 파라미터에 기초하여 작업 키를 생성함으로써 개선될 수 있다. 보안 파라미터(들)는 디바이스 상에서 인증될 소프트웨어 및/또는 무선 디바이스

(뒷면에 계속)

*대 표 도* - 도6



에 대한 보안의 다른 양상들과 관련될 수 있다. 보안 파라미터(들)는 소프트웨어가 허가되는지 여부 및/또는 소프트웨어에 대해 허가된 적어도 하나의 동작 기능을 표시할 수 있다. 적어도 하나의 보안 기능은 작업 키에 기초하여 디바이스에 대해 수행될 수 있다. 예를 들어, 작업 키는 디바이스에 대한 데이터를 암호화, 서명, 암호화해제 또는 검증하는데 이용될 수 있다. 작업 키는 적어도 하나의 보안 기능을 위해 소프트웨어에 의해 직접적으로 또는 간접적으로 이용될 수 있다.

(52) CPC특허분류
***G06F 21/575*** (2013.01)
***G06F 21/79*** (2013.01)
***H04L 63/123*** (2013.01)
***H04L 9/3247*** (2013.01)
***H04W 12/10*** (2021.01)
***H04W 12/12*** (2021.01)
***H04W 88/02*** (2013.01)
*H04L 2463/061* (2013.01)

(56) 선행기술조사문헌
US20120201379 A1*
US20060117181 A1
US20030163719 A1
JP2008152764 A
*는 심사관에 의하여 인용된 문헌

# 명 세 서

## 청구범위

### 청구항 1

보안을 제공하는 방법으로서,

소프트웨어에 의해, 디바이스의 비밀 키 및 보안 파라미터들의 세트 중 적어도 하나의 보안 파라미터에 기초하여 작업 키를 생성하는 단계 - 상기 보안 파라미터들의 세트 및 상기 비밀 키는 적어도 2개의 상이한 엔티티들에 의해 상기 디바이스 상에 프로비저닝(provision)되고 그리고 저장되며, 상기 소프트웨어는 상기 보안 파라미터들의 세트에 따라 상기 디바이스 상에서의 실행이 허가되고, 상기 적어도 하나의 보안 파라미터는 상기 디바이스 상에서의 상기 소프트웨어에 대해 허가된 적어도 하나의 동작 기능(operating function)을 결정함 - ; 및

상기 작업 키에 기초하여 상기 디바이스에 대한 적어도 하나의 보안 기능을 수행하는 단계를 포함하고,

상기 작업 키는 상기 적어도 하나의 보안 기능을 위해 직접적으로 또는 간접적으로 이용되는,

보안을 제공하는 방법.

### 청구항 2

제 1 항에 있어서,

상기 적어도 하나의 보안 파라미터는 상기 소프트웨어가 상기 디바이스에 대해 허가되는지 여부를 결정하는데 이용되는 공개 키를 포함하는,

보안을 제공하는 방법.

### 청구항 3

제 2 항에 있어서,

상기 공개 키는 상기 소프트웨어를 서명(sign)하는데 이용되는 개인 키에 대응하는,

보안을 제공하는 방법.

### 청구항 4

제 1 항에 있어서,

상기 비밀 키 및 상기 적어도 하나의 보안 파라미터는 상이한 시간들에서 상기 디바이스로 로딩되는,

보안을 제공하는 방법.

### 청구항 5

제 1 항에 있어서,

상기 작업 키를 생성하는 단계는 키 유도 함수를 이용하여 상기 디바이스의 상기 비밀 키 및 상기 적어도 하나의 보안 파라미터에 기초하여 상기 작업 키를 생성하는 단계를 포함하는,

보안을 제공하는 방법.

### 청구항 6

제 1 항에 있어서,

상기 적어도 하나의 보안 기능을 수행하는 단계는 상기 작업 키를 이용하여 상기 디바이스에 대한 데이터를 암호화하거나 또는 서명하는 단계를 포함하는,

보안을 제공하는 방법.

**청구항 7**

제 1 항에 있어서,

상기 적어도 하나의 보안 기능을 수행하는 단계는 상기 작업 키를 이용하여 상기 디바이스에 대한 데이터를 암호화해제하거나 또는 검증하는 단계를 포함하는,

보안을 제공하는 방법.

**청구항 8**

제 1 항에 있어서,

상기 적어도 하나의 보안 기능을 수행하는 단계는 상기 소프트웨어의 제어 하에 상기 적어도 하나의 보안 기능을 수행하는 단계를 포함하는,

보안을 제공하는 방법.

**청구항 9**

제 1 항에 있어서,

보안 메커니즘을 통해 상기 소프트웨어를 인증하지 않고 상기 디바이스 상의 소프트웨어를 실행하는 단계를 더 포함하는,

보안을 제공하는 방법.

**청구항 10**

제 1 항에 있어서,

상기 디바이스 상의 보안 메모리에 상기 비밀 키를 저장하는 단계; 및

상기 디바이스 상의 상기 보안 메모리 또는 비보안 메모리에 상기 적어도 하나의 보안 파라미터를 저장하는 단계를 더 포함하는,

보안을 제공하는 방법.

**청구항 11**

소프트웨어에 의해, 디바이스의 비밀 키 및 보안 파라미터들의 세트 중 적어도 하나의 보안 파라미터에 기초하여 작업 키를 생성하기 위한 수단 - 상기 보안 파라미터들의 세트 및 상기 비밀 키는 적어도 2개의 상이한 엔티티들에 의해 상기 디바이스 상에 프로비저닝(provision)되고 그리고 저장되며, 상기 소프트웨어는 상기 보안 파라미터들의 세트에 따라 상기 디바이스 상에서의 실행이 허가되고, 상기 적어도 하나의 보안 파라미터는 상기 디바이스 상에서의 상기 소프트웨어에 대해 허가된 적어도 하나의 동작 기능을 결정함 - ; 및

상기 작업 키에 기초하여 상기 디바이스에 대한 적어도 하나의 보안 기능을 수행하기 위한 수단을 포함하고,

상기 작업 키는 상기 적어도 하나의 보안 기능을 위해 직접적으로 또는 간접적으로 이용되는,

장치.

**청구항 12**

제 11 항에 있어서,

상기 비밀 키 및 상기 적어도 하나의 보안 파라미터는 상이한 시간들에서 상기 디바이스로 로딩되는,

장치.

**청구항 13**

제 11 항에 있어서,

상기 적어도 하나의 보안 기능을 수행하기 위한 수단은 상기 소프트웨어를 인증하기 위한 보안 메커니즘의 활성

화 이전에 상기 적어도 하나의 보안 기능을 수행하기 위한 수단을 포함하는,

장치.

**청구항 14**

디바이스에 대한 소프트웨어를 저장하도록 구성되는 메모리; 및

상기 메모리에 커플링되는 프로세서를 포함하고,

상기 프로세서는:

소프트웨어에 의해, 상기 디바이스의 비밀 키 및 보안 파라미터들의 세트 중 적어도 하나의 보안 파라미터에 기초하여 작업 키를 생성하고 - 상기 보안 파라미터들의 세트 및 상기 비밀 키는 적어도 2개의 상이한 엔티티들에 의해 상기 디바이스 상에 프로비저닝(provision)되고 그리고 저장되며, 상기 소프트웨어는 상기 보안 파라미터들의 세트에 따라 상기 디바이스 상에서의 실행이 허가되고, 상기 적어도 하나의 보안 파라미터는 상기 디바이스 상에서의 상기 소프트웨어에 대해 허가된 적어도 하나의 동작 기능을 결정함 - ; 그리고

상기 작업 키에 기초하여 상기 디바이스에 대한 적어도 하나의 보안 기능을 수행하도록 구성되고,

상기 작업 키는 상기 적어도 하나의 보안 기능을 위해 직접적으로 또는 간접적으로 이용되는,

장치.

**청구항 15**

제 14 항에 있어서,

상기 비밀 키 및 상기 적어도 하나의 보안 파라미터는 상이한 시간들에서 상기 디바이스로 로딩되는,

장치.

**청구항 16**

제 14 항에 있어서,

상기 프로세서는 상기 소프트웨어를 인증하기 위한 보안 메커니즘의 활성화 이전에 상기 적어도 하나의 보안 기능을 수행하도록 구성되는,

장치.

**청구항 17**

비-일시적 컴퓨터-판독가능 저장 매체로서,

적어도 하나의 컴퓨터로 하여금, 소프트웨어에 의해, 디바이스의 비밀 키 및 보안 파라미터들의 세트 중 적어도 하나의 보안 파라미터에 기초하여 작업 키를 생성하게끔 하기 위한 코드 - 상기 보안 파라미터들의 세트 및 상기 비밀 키는 적어도 2개의 상이한 엔티티들에 의해 상기 디바이스 상에 프로비저닝(provision)되고 그리고 저장되며, 상기 소프트웨어는 상기 보안 파라미터들의 세트에 따라 상기 디바이스 상에서의 실행이 허가되고, 상기 적어도 하나의 보안 파라미터는 상기 디바이스 상에서의 상기 소프트웨어에 대해 허가된 적어도 하나의 동작 기능을 결정함 - ; 및

상기 적어도 하나의 컴퓨터로 하여금, 상기 작업 키에 기초하여 상기 디바이스에 대한 적어도 하나의 보안 기능을 수행하게끔 하기 위한 코드를 포함하고,

상기 작업 키는 상기 적어도 하나의 보안 기능을 위해 직접적으로 또는 간접적으로 이용되는,

비-일시적 컴퓨터-판독가능 저장 매체.

**청구항 18**

제 17 항에 있어서,

상기 비밀 키 및 상기 적어도 하나의 보안 파라미터는 상이한 시간들에서 상기 디바이스로 로딩되는,

비-일시적 컴퓨터-판독가능 저장 매체.

**청구항 19**

제 17 항에 있어서,

상기 적어도 하나의 컴퓨터로 하여금, 적어도 하나의 보안 기능을 수행하게끔 하기 위한 코드는, 상기 적어도 하나의 컴퓨터로 하여금, 상기 소프트웨어를 인증하기 위한 보안 메커니즘의 활성화 이전에 상기 적어도 하나의 보안 기능을 수행하게끔 하기 위한 코드를 포함하는,

비-일시적 컴퓨터-판독가능 저장 매체.

**청구항 20**

삭제

**청구항 21**

삭제

**청구항 22**

삭제

## *발명의 설명*

### *기 술 분 야*

[0001] [0001] 본 개시는 일반적으로 전자기기들에 관한 것으로, 더 구체적으로는, 전자 디바이스 상에서 보안을 제공하기 위한 기법들에 관한 것이다.

### *배 경 기 술*

[0002] [0002] 전자 디바이스(예를 들어, 셀룰러 폰 또는 스마트폰)는 전형적으로 디바이스 상에서의 하드웨어의 동작을 제어하고 디바이스의 다양한 기능들을 지원하는 소프트웨어에 기초하여 동작한다. 보안 메커니즘(예를 들어, 보안 부트)은 디바이스에 대해 허가된 소프트웨어만이 디바이스 상에서 실행될 수 있음을 보장하기 위해 이용될 수 있다. 그러나, 디바이스는 디바이스 상에서의 보안 메커니즘의 활성화 이전에 악성 공격(예를 들어, 제조 동안)에 취약할 수 있다. 이러한 취약한 시간 기간 동안, 허가되지 않은 소프트웨어는 디바이스 상에서 보안 정보(예를 들어, 보안 키들)에 액세스하기 위해 그리고/또는 보안 정보를 이용하여 데이터를 조작하기 위해 악성으로 디바이스로 로딩되고 디바이스에 의해 실행될 수 있다.

### *발명의 내용*

[0003] [0003] 전자 디바이스의 보안을 개선하기 위한 기법들이 본원에 개시된다. 본 개시의 양상에서, 디바이스의 보안은 디바이스의 하드웨어 비밀 키뿐만 아니라 적어도 하나의 보안 파라미터에 기초하여 작업 키를 생성함으로써 개선될 수 있다. (하드웨어 비밀 키 대신에) 작업 키가 디바이스에 대한 보안 기능들을 수행(예를 들어, 데이터를 암호화 및 암호화해제)하는데 이용될 수 있다.

[0004] [0004] 예시적 설계에서, 작업 키는, 예를 들어, 키 유도 함수를 이용하여 디바이스의 적어도 하나의 보안 파라미터 및 비밀 키에 기초하여 생성될 수 있다. 적어도 하나의 보안 파라미터는 디바이스 상에서 인증될 소프트웨어 및/또는 디바이스에 대한 보안의 다른 양상들과 관련될 수 있다. 적어도 하나의 보안 기능은 작업 키에 기초하여 디바이스에 대해 수행될 수 있다. 예를 들어, 작업 키는 디바이스에 대한 데이터를 암호화, 서명(sign), 암호화해제 또는 검증하는데 이용될 수 있다. 작업 키는 적어도 하나의 보안 기능을 위해 소프트웨어에 의해 직접적으로 또는 간접적으로 이용될 수 있다.

[0005] [0005] 적어도 하나의 보안 파라미터는 디바이스에 대한 보안의 다양한 양상들을 제어할 수 있다. 예를 들어, 적어도 하나의 보안 파라미터는 소프트웨어가 디바이스 상에서의 실행에 대해 허가되는지 여부, 적어도 하나의 동작 기능이 소프트웨어에 대해 허가되는지 여부 등을 결정할 수 있다. 하나의 설계에서, 적어도 하나의 보안 파라미터는 소프트웨어가 디바이스에 대해 허가되는지 여부를 결정하는데 이용되는 공개 키를 포함할 수 있다.

공개 키는 소프트웨어를 서명하는데 이용되는 개인 키에 대응할 수 있다. 적어도 하나의 보안 파라미터는 또한 다른 타입들의 정보를 포함할 수 있다.

[0006] [0006] 본 개시의 다양한 양상들 및 특징들이 아래에 추가로 상세하게 설명된다.

## 도면의 간단한 설명

[0007] [0007] 도 1은 무선 디바이스의 블록도를 도시한다.

[0008] [0008] 도 2는 무선 디바이스에 대한 예시적 제조 프로세스를 도시한다.

[0009] [0009] 도 3a는 무선 디바이스 상에 보안 정보를 저장하기 위한 프로세스를 도시한다.

[0010] [0010] 도 3b는 무선 디바이스의 보안 부트(secure boot)를 수행하기 위한 프로세스를 도시한다.

[0011] [0011] 도 4는 하드웨어 비밀 키에 기초하여 데이터를 암호화 및 암호화해제하기 위한 프로세스를 도시한다.

[0012] [0012] 도 5는 작업 키에 기초하여 데이터를 암호화 및 암호화해제하기 위한 프로세스를 도시한다.

[0013] [0013] 도 6은 디바이스에 대한 보안을 제공하기 위한 프로세스를 도시한다.

## 발명을 실시하기 위한 구체적인 내용

[0008] [0014] 본원에 개시된 보안 키 생성 기법들은 무선 통신 디바이스들, 핸드헬드 디바이스들, 게임 디바이스들, 컴퓨팅 디바이스들, 소비자 전자 디바이스들, 컴퓨터들 등과 같은 다양한 전자 디바이스들에 대해 이용될 수 있다. 명료함을 위해, 기법들은 무선 통신 디바이스에 대해 아래에 설명된다.

[0009] [0015] 도 1은 본원에 개시된 보안 키 생성 기법들을 구현할 수 있는 무선 통신 디바이스(100)의 예시적 설계의 블록도를 도시한다. 무선 디바이스(100)는 셀룰러 폰, 스마트폰, 태블릿, 무선 모뎀, PDA(personal digital assistant), 핸드헬드 디바이스, 랩탑 컴퓨터, 스마트북, 네트북, 코드리스 폰, WLL(wireless local loop) 스테이션, 블루투스 디바이스 등일 수 있다. 무선 디바이스(100)는 하나 또는 둘 이상의 무선 통신 시스템들과의 양방향 통신을 지원할 수 있다.

[0010] [0016] 데이터 송신을 위해, 디지털 모듈(120)은 송신될 데이터를 프로세싱(예를 들어, 인코딩 및 변조)하고, 출력 기저대역 신호를 송신기(TMTR)(114)에 제공할 수 있다. 송신기(114)는 안테나(112)를 통해 기지국들에 송신될 수 있는 출력 RF(radio frequency) 신호를 생성하기 위해 출력 기저대역 신호를 증폭, 필터링 및 업컨버팅할 수 있다.

[0011] [0017] 데이터 수신을 위해, 안테나(112)는 기지국들 및/또는 다른 송신기 스테이션들로부터 신호들을 수신할 수 있으며, 수신된 RF 신호를 수신기(RCVR)(116)에 제공할 수 있다. 수신기(116)는 RF로부터 기저대역으로 수신된 RF 신호를 다운컨버팅하고, 다운컨버팅된 신호를 필터링하고 증폭시키며, 입력 기저대역 신호를 디지털 모듈(120)에 제공할 수 있다. 디지털 모듈(120)은 무선 디바이스(100)에 전송된 데이터를 복원하기 위해 입력 기저대역 신호를 프로세싱(예를 들어, 복조 및 디코딩)할 수 있다.

[0012] [0018] 디지털 모듈(120)은 무선 디바이스(100)에 대한 디지털 프로세싱을 지원하기 위해 다양한 프로세싱, 인터페이스 및 메모리 유닛들을 포함할 수 있다. 도 1에 도시된 설계에서, 디지털 모듈(120)은 모뎀 프로세서(122), CPU(central processing unit)/RISC(reduced instruction set computer) 프로세서(124), 메인 제어기(126), 내부 메모리(130), 보안 메모리(140), 메모리 제어기(148) 및 I/O(input/output) 제어기(158)를 포함하고, 이들 모두는 하나 또는 둘 이상의 데이터 버스들(160)을 통해 서로 간에 통신할 수 있다.

[0013] [0019] 모뎀 프로세서(122)는 데이터 송신 및 수신에 대한 프로세싱, 예를 들어, 인코딩, 변조, 복조, 디코딩 등을 수행할 수 있다. CPU/RISC 프로세서(124)는 무선 디바이스(100)에 대한 범용 프로세싱, 예를 들어, 오디오, 비디오, 그래픽들 및/또는 다른 애플리케이션들에 대한 프로세싱을 수행할 수 있다. 메인 제어기(126)는 디지털 모듈(120) 내의 다양한 유닛들의 동작을 지시(direct)할 수 있다. 내부 메모리(130)는 디지털 모듈(120) 내의 제어기들 및 프로세서들에 의해 이용되는 소프트웨어(132) 및/또는 데이터를 저장할 수 있다. 메모리(130)는 SRAM(static random access memory) 또는 다른 타입들의 메모리로 구현될 수 있다.

[0014] [0020] 보안 메모리(140)는 보안 키들(142), 보안 파라미터들(144), 부트 코드(146) 및/또는 다른 보안 정보를 저장할 수 있다. 보안 키들(142)은, 예를 들어, 무선 디바이스(100)에 의해 전송된 데이터의 암호화, 무선 디바이스(100)에 전송된 암호화된 데이터의 암호화해제, 내부 메모리(130)로 로딩된 소프트웨어의 인증 등을 위해

무선 디바이스(100)에 대한 보안 기능들을 위해 이용될 수 있다. 보안 파라미터들(144)은 무선 디바이스(100)의 보안과 관련된 다양한 양상들을 제어할 수 있다. 부트 코드(146)는 무선 디바이스(100)로 로딩되는 소프트웨어를 인증하기 위해 보안 부트를 수행할 수 있다. 메모리(140)는 ROM(read-only memory), OTP(one-time programmable) 엘리먼트들 및/또는 다른 타입들의 메모리로 구현될 수 있다.

[0015] [0021] 메모리 제어기(148)는 외부 메모리(150)와 디지털 모듈(120) 사이의 데이터의 전달을 가능하게 할 수 있다. 외부 메모리(150)는 디지털 모듈(120) 내의 프로세싱 유닛들에 대한 대용량/벌크 저장을 제공할 수 있다. 예를 들어, 메모리(150)는 실행을 위해 디지털 모듈(120)로 로딩될 수 있는 소프트웨어(152), 데이터 등을 저장할 수 있다. 메모리(150)는 (i) NAND 플래시 및/또는 NOR 플래시 메모리와 같은 벌크 비-휘발성 메모리, (ii) SDRAM(synchronous dynamic random access memory) 또는 DRAM(dynamic random access memory)과 같은 벌크 휘발성 메모리 및/또는 (iii) 다른 타입들의 메모리를 포함할 수 있다. I/O 제어기(158)는 무선 디바이스(100)가 보안 서버들 및/또는 다른 엔티티들과 통신하게 할 수 있다.

[0016] [0022] 도 1은 디지털 모듈(120)의 예시적 설계를 도시한다. 일반적으로, 디지털 모듈(120)은 임의의 수의 프로세싱, 인터페이스 및 메모리 유닛들을 포함할 수 있다. 디지털 모듈(120)은 또한, 하나 또는 둘 이상의 DSP(digital signal processor)들, 마이크로-프로세서들, RISC 프로세서들 등으로 구현될 수 있다. 디지털 모듈(120)은 하나 또는 둘 이상의 ASIC(application specific integrated circuit)들 및/또는 다른 IC(integrated circuit)들로 구현될 수 있다.

[0017] [0023] 무선 디바이스(100)와 같은 전자 디바이스는 전형적으로, 일련의 제조 단계들을 고려한다. 전자 디바이스는 하나 또는 둘 이상의 제조 단계들 동안 보안 공격에 취약할 수 있다.

[0018] [0024] 도 2는 무선 디바이스(100)(또는 임의의 전자 디바이스)에 대한 예시적 제조 프로세스(200)를 도시한다. 키 프로비저닝 엔티티는 하드웨어(HW) 비밀 키를 무선 디바이스(100) 상에 보안적으로 프로비저닝할 수 있다(단계 1). 키 프로비저닝 엔티티는 무선 디바이스(100)(도 2에 도시된 바와 같음) 또는 일부 다른 엔티티에서 이용되는 IC(integrated circuit) 칩(예를 들어, ASIC)의 IC 칩 제조사일 수 있다. 하드웨어 비밀 키는 무선 디바이스(100) 상의 보안 메모리(140)에 저장될 수 있다.

[0019] [0025] 디바이스 제조사(device manufacturer)는 제조된 디바이스들로의 액세스가 단지 신뢰성 있는 직원들에만 제한될 수 없는 보안되지 않은 제조 환경에서 무선 디바이스(100)를 제조 또는 구축할 수도 있다. 디바이스 제조사는 ODM(original device manufacturer)(도 2에 도시되는 바와 같음), OEM(original equipment manufacturer), 또는 무선 디바이스(100)를 구축, 어셈블(assemble) 및 프로비저닝하는 임의의 엔티티일 수 있다. 디바이스 제조사는 전형적으로, 소프트웨어를 로딩하고, 보안 파라미터들을 로딩하며, 무선 디바이스(100)에 대한 보안 기능들을 인에이블한다(단계 2).

[0020] [0026] 보안 서버는 하드웨어 비밀 키를 이용하여 비밀 데이터를 무선 디바이스(100)에 프로비저닝할 수 있다(단계 3). 보안 데이터 프로비저닝은 전형적으로, 보안 설비에서, 비밀 데이터를 무선 디바이스(100)로 로딩하도록 수행된다. 보안 데이터 프로비저닝을 위해, 보안 서버는 하드웨어 비밀 키를 이용하여 무선 디바이스(100)와 데이터를 보안적으로 교환할 수 있다. 프로비저닝된 비밀 데이터는 무선 디바이스(100) 상의 보안 메모리(140)에 저장될 수 있다.

[0021] [0027] 도 2에 도시된 바와 같이, 보안 파라미터들은 제조 프로세스 동안 무선 디바이스(100)로 로딩될 수 있다. 보안 파라미터들은 무선 디바이스(100)에 대한 보안의 다양한 양상들을 제어할 수 있으며, 다음의 것들 중 하나 또는 둘 이상을 포함할 수 있다:

[0022] · 디바이스의 RoT(root-of-trust)와 관련된 정보,

[0023] · 어떤 소프트웨어가 디바이스 상에서 실행될 수 있는지 그리고/또는 소프트웨어가 디바이스 상에서 어떻게 동작할 수 있는지를 제어하는 정보,

[0024] · 특정 보안 피처들이 디바이스 상에서 인에이블될 수 있는지 아니면 디스에이블될 수 있는지를 제어하는 정보, 및/또는

[0025] · 다른 보안 관련 정보.

[0026] [0028] 보안 파라미터들은 무선 디바이스(100)의 RoT(root-of-trust)와 관련된 정보를 포함할 수 있다. RoT(root-of-trust)는 무선 디바이스(100)에 대한 모든 보안 메커니즘들의 근본적 기초(foundation basis)일 수 있다. RoT(root-of-trust) 관련 정보는 하나 또는 둘 이상의 개인 루트 키들에 대응하는 하나 또는 둘 이상

의 공개 루트 키들, 공개 루트 키(들)에 대한 하나 또는 둘 이상의 인증서들 등을 포함할 수 있다. 개인 루트 키는 무선 디바이스(100)에 전송된 데이터를 서명하는데 이용될 수 있다. 대응하는 공개 루트 키는 개인 루트 키로 서명된 데이터를 인증하는데 이용될 수 있다. 예를 들어, 공개 루트 키는 아래에 설명되는 바와 같이, 무선 디바이스(100)로 로딩된 소프트웨어를 인증하기 위해 보안 부트에서 이용될 수 있다.

[0027] [0029] 보안 파라미터들은 어떤 소프트웨어가 무선 디바이스(100) 상에서 실행될 수 있는지 그리고/또는 소프트웨어가 무선 디바이스(100) 상에서 어떻게 동작할 수 있는지를 제어할 수 있다. 예를 들어, 보안 파라미터들은 무선 디바이스(100) 상에서의 실행에 대해 허가된 소프트웨어를 인증하는데 이용되는 공개 키를 포함할 수 있다. 소프트웨어는 공개 키에 대응하는 개인 키에 기초하여 서명될 수 있으며, 무선 디바이스(100) 상에 저장될 수 있다. 소프트웨어는, 아래에서 설명되는 바와 같이, 무선 디바이스(100) 상에서의 실행 이전에 공개 키에 기초하여 인증될 수 있다.

[0028] [0030] 보안 파라미터들은 특정 보안 피처들이 무선 디바이스(100) 상에서 인에이블될 수 있는지 아니면 디스에이블될 수 있는지를 제어할 수 있다. 예를 들어, 보안 파라미터들은 무선 디바이스(100)의 보안 부트가 인에이블되는지 여부, 테스팅 또는 디버그 동안 무선 디바이스(100)의 내부 상태들로의 액세스를 허용하기 위해 무선 디바이스(100)의 디버그 능력이 디스에이블될 수 있는지 여부 등을 제어할 수 있다.

[0029] [0031] 일부 보안 파라미터들은 다수의 목적들을 제공할 수 있다. 예를 들어, 공개 루트 키는 어떤 소프트웨어가 무선 디바이스(100) 상에서 실행될 수 있는지를 제어하는 것뿐만 아니라 무선 디바이스(100)의 RoT(root-of-trust) 둘 모두로서의 역할을 할 수 있다.

[0030] [0032] 보안 파라미터들은 무선 디바이스(100) 상의 보안 메모리(140)에 저장될 수 있다. 예를 들어, 보안 파라미터들은 무선 디바이스(100)에 대한 프로세서의 IC 칩 상의 OTP 엘리먼트들을 이용하여 저장될 수 있다. OTP 엘리먼트들은 퓨즈들의 상태를 통해 데이터를 영구적으로 저장하기 위해 제조 동안 1회 블로우(blow)될 수 있는 퓨즈들로 구현될 수 있다.

[0031] [0033] 소프트웨어 및 보안 정보는 소프트웨어의 실행 이전에 무선 디바이스(100)가 소프트웨어를 인증하도록 허용하는 방식으로 무선 디바이스(100) 상에 저장될 수 있다. 무선 디바이스(100) 상에 저장된 소프트웨어를 인증하기 위한 예시적 보안 메커니즘이 아래에서 설명된다.

[0032] [0034] 도 3a는 무선 디바이스(100)로 로딩된 소프트웨어의 인증을 지원하기 위해 무선 디바이스(100) 상에 보안 정보를 저장하기 위한 프로세서(300)의 예시적 설계를 도시한다. 프로세스(300)는 보안 서버 또는 일부 다른 엔티티에 의해 수행될 수 있다.

[0033] [0035] 보안 서버에서, 서명 함수(320)는 공개 키 X' 상에서 디지털 시그니처 SR을 생성하고, 가능하게는, 개인 루트 키 R을 이용하여 다른 정보를 생성할 수 있다. 시그니처 SR은 보안 서버인 소스 엔티티를 인증하는데 이용될 수 있다. 서명 함수(320)는 RSA(Rivest, Shamir and Adleman) 알고리즘, DSA(Digital Signature Algorithm) 또는 일부 다른 암호법(cryptographic)(디지털 시그니처 또는 암호화) 알고리즘을 구현할 수 있다. 인증서 생성기(322)는 공개 키 X', 시그니처 SR, 및 가능하게는, 다른 정보, 이를테면, 소스 엔티티의 식별자, 이용하도록 선택되는 암호법 알고리즘, 인증서의 만료일 등을 포함하는 인증서 CR을 형성할 수 있다. 이러한 인증서는 무선 디바이스(100) 상의 보안 메모리(140)(또는 일부 다른 메모리)에서 X.509 인증서로서 저장될 수 있다. 공개 루트 키 R'는 보안 방식으로 무선 디바이스(100)에 이용가능해질 것이며, 무선 디바이스(100) 상의 보안 메모리(140)(예를 들어, OTP 메모리 또는 ROM)에 저장될 수 있다.

[0034] [0036] 보안 해쉬 함수(330)는 무선 디바이스(100)로 로딩되는 소프트웨어를 해쉬할 수 있으며, 해쉬 디지스트 S를 제공할 수 있다. 보안 해쉬 함수(330)는 SHA-1, SHA-2, MD-5 또는 일부 다른 보안 해쉬 알고리즘을 구현할 수 있다. 서명 함수(332)는 개인 키 X를 이용하여 디지스트 S 상에서 디지털 시그니처 SX를 생성할 수 있다. 시그니처 SX는 메모리(150)에 저장될 수 있다. 서명 함수(332)는 RSA, DSA 또는 일부 다른 암호법 알고리즘을 구현할 수 있다. 소프트웨어는 무선 디바이스(100) 상의 메모리(150)(또는 일부 다른 메모리)에 저장될 수 있다.

[0035] [0037] 도 3b는 무선 디바이스(100)의 보안 부트에 대한 프로세스(350)의 예시적 설계를 도시한다. 프로세스(350)는 아래에서 설명되는 바와 같이, 무선 디바이스(100)에 의해 수행될 수 있다. 무선 디바이스(100)에서, 검증 함수(370)는 보안 메모리(140)로부터 인증서 CR 및 공개 루트 키 R'을 수신할 수 있다. 검증 함수(370)는 인증서 CR로부터 시그니처 SR 및 공개 키 X'를 추출하고, 공개 루트 키 R'로 시그니처 SR을 검증하고, 시그니처 SR이 검증되는 경우 공개 키 X'를 제공할 수 있다. 제 3 자에 의한 인증서 CR에 대한 임의의 탬퍼링

(tampering)은 검증되지 않은 시그니처 SR에 의해 쉽게 검출될 수 있다.

[0036] [0038] 보안 해쉬 함수(380)는 메모리(150)로부터 소프트웨어를 수신하고, 소프트웨어를 해쉬하고, 해쉬 디지스트 S'를 제공할 수 있다. 보안 해쉬 함수(380)는 도 3a의 보안 해쉬 함수(330)에 의해 이용되는 동일한 보안 해쉬 알고리즘을 구현할 수 있다. 검증 함수(390)는 보안 해쉬 함수(380)로부터 디지스트 S'를 수신하고, 메모리(150)로부터 디지털 시그니처 SX를 수신하고, 검증 함수(370)로부터 공개 키 X'를 수신할 수 있다. 검증 함수(390)는 공개 키 X' 및 디지스트 S'로 디지털 시그니처 SX를 검증할 수 있으며, 디지털 시그니처 SX가 검증되는지 아닌지를 표시할 수 있다. 공개 키 X'는 공개 루트 키 R'로 인증될 수 있다. 따라서, 제 3 자에 의한 디지털 시그니처 SX 및/또는 소프트웨어에 대한 임의의 탬퍼링은 검증되지 않은 디지털 시그니처 SX에 의해 쉽게 검출될 수 있다. 디지털 시그니처 SX가 검증되는 경우, 소프트웨어는 이용을 위해 제공될 수 있다. 그렇지 않으면, 에러 메시지가 제공될 수 있다.

[0037] [0039] 도 3a는 예시적 보안 부트 소프트웨어 서명 프로세스를 도시한다. 도 3b는 예시적 보안 부트 소프트웨어 인증 프로세스를 도시한다. 보안 부트는 또한 다른 방식들로 구현될 수 있다.

[0038] [0040] 정상 동작 동안, 무선 디바이스(100)는 소프트웨어의 실행 이전에 무선 디바이스(100)로 로딩되는 소프트웨어를 인증하기 위해 보안 부트를 수행할 수 있다. 보안 부트에 대해, 무선 디바이스(100)는 먼저, 공개 키 X'의 진위성(authenticity)을 결정하기 위해 공개 루트 키 R'로 시그니처 SR을 인증할 수 있다. 공개 키 X'가 인증된 이후, 무선 디바이스(100)는 소프트웨어의 진위성을 결정하기 위해 공개 키 X'로 시그니처 SX를 인증할 수 있다. 보안 부트는 무선 디바이스(100)에 대해 허가된 소프트웨어만이 무선 디바이스(100) 상에서 실행될 수 있음을 보장할 수 있다.

[0039] [0041] 하드웨어 비밀 키들은 SoC(system-on-chip) IC들과 같은 ASIC들 상에서 공통으로 프로비저닝되고, ASIC들 외부의 메모리들에 저장된 데이터를 암호화 및 암호화해제하는데 이용된다. 이 보안 메커니즘은 또한 보안 파일 시스템 또는 암호화된 파일 시스템으로서 공지된다. 하드웨어 비밀 키들은 전형적으로 공개/개인 키들과 구분된다. 하드웨어 비밀 키는 전형적으로, 디바이스에서 비밀들을 암호화 및 암호화해제하는데 이용되는 대칭 키이다. 예를 들어, 하드웨어 비밀 키는 SSD(solid state disk), MMC(MultiMediaCard), eMMC 등과 같은 보호되지 않은 데이터 저장소에 암호화된 데이터를 저장하기 이전에 데이터를 암호화하는데 이용될 수 있다. 많은 OEM들은 그들의 제조 현장(floor) 직원들 또는 ODM 직원들을 신뢰하지 않는다. 따라서, 대부분의 보안 구현들은 소프트웨어가 ASIC 상의 하드웨어 비밀 키로 액세스하게 허용하지 않는다. 그러나, 이러한 보안 구현들은 전형적으로, 하드웨어 비밀 키가 소프트웨어에 의해 간접적으로 이용되게 허용한다. 이러한 이용은 데이터의 암호화해제 또는 암호화를 포함할 수 있다.

[0040] [0042] 소프트웨어는 그것이 ASIC의 RoT(root-of-trust)와 관련 있는 인증 메커니즘에 의해 인증되고 검증된 이후 신뢰성 있는 것으로 고려될 수 있다. 이러한 인증 메커니즘은 전형적으로 보안 부트로 지칭된다. 그러나, 보안 부트는 제조 프로세스 동안 이용가능하지 않을 수 있다.

[0041] [0043] 하드웨어 비밀 키가 프로비저닝되고, 보안 부트가 인에이블되지 않으며, RoT(root-of-trust)가 프로비저닝되지 않은 일반적 ASIC을 OEM/ODM에 제공하는 것이 통상적 관행(common practice)이다. 하드웨어 비밀 키는 디바이스 또는 ASIC 상의 보안 메모리에 프로비저닝될 수 있다. 이러한 스테이지에서, 디바이스 상의 소프트웨어의 무결성을 보호할 수 있는 보안 부트 및/또는 다른 보안 메커니즘들을 인에이블하기 이전에, 허가되지 않은 소프트웨어가 디바이스로 로딩되고 디바이스에 의해 실행될 수 있다. 디바이스 상에 프로비저닝된 임의의 보안 키는 허가되지 않은 소프트웨어에 의해 조작될 수도 있다. 이것은, 신뢰성 없는 ODM/OEM 제조 직원들이, 하드웨어 비밀 키를 이용하여 데이터를 조작하거나, 기밀 정보를 노출하거나, 또는 하드웨어 비밀 키에 의해 보호되는 데이터의 무결성을 절충하게 하는 길을 열어준다.

[0042] [0044] 따라서, 무선 디바이스(100)는 (i) 하드웨어 비밀 키가, 예를 들어, 도 2의 단계 1에서 IC 칩 제조사에 의해 무선 디바이스(100) 상에서 프로비저닝되는 시기로부터 (ii) 보안이, 예를 들어, 도 2의 단계 3에서 OEM에 의해 무선 디바이스(100) 상에서 락킹되는(locked) 시기에 공격에 취약할 수 있다. 이러한 취약한 시간 기간 동안, 허가되지 않은 소프트웨어는, 예를 들어, 하드웨어 비밀 키가 무선 디바이스(100) 상의 소프트웨어에 의해 액세스가능하지 않은 경우들에서, (i) 하드웨어 비밀 키에 액세스하고 그리고/또는 (ii) 하드웨어 비밀 키를 이용하여 데이터를 조작하기 위해, 악성으로 무선 디바이스(100)로 로딩되고 무선 디바이스에 의해 실행될 수 있다.

[0043] [0045] 본 개시의 양상에서, 디바이스의 보안은 하드웨어 비밀 키뿐만 아니라 적어도 하나의 보안 파라미터에

기초하여 작업 키를 생성함으로써 개선될 수 있으며(그리고 위에서 설명된 보안 취약성(weakness)이 효과적으로 처리될 수 있음), 이는 디바이스에 대해 허가된 소프트웨어와 관련될 수 있다. (하드웨어 비밀 키 대신에) 작업 키는 디바이스 상에서 데이터를 암호화 및/또는 암호화해제하는데 이용될 수 있다.

[0044] [0046] 도 4는 하드웨어 비밀 키에 기초하여 종래의 방식으로 데이터를 암호화 및 암호화해제하기 위한 프로세스(400)를 도시한다. 보안 서버(410)(OEM에 속할 수 있음)에서, 암호 엔진(430)은 디바이스(450)의 하드웨어 비밀 키(442)로 데이터를 암호화하여 암호화된 데이터를 획득할 수 있다. 암호 엔진(430)은 보안 서버(410) 내의 소프트웨어(440)에 의해 지시되는 대로 동작할 수 있다. 암호화된 데이터는 디바이스(450)에 전송될 수 있다.

[0045] [0047] 디바이스(450)에서, 암호 엔진(470)은 보안 서버(410)로부터 암호화된 데이터를 수신할 수 있으며, 디바이스(450)의 하드웨어 비밀 키(442)로 암호화된 데이터를 암호화해제할 수 있다. 암호 엔진(470)은 디바이스(450) 내의 소프트웨어(480)에 의해 지시되는 대로 동작할 수 있다. 위에서 기술된 바와 같이, 소프트웨어(480)는 디바이스(450) 상에서의 보안 부트의 인에이블 이전에 불안전(insecure)할 수 있다. 이러한 경우, 악성 소프트웨어가 디바이스(450)로 로딩될 수 있으며, (i) 암호화된 데이터를 암호화해제하도록 암호 엔진(470)에 지시하고 그리고/또는 (ii) 암호화해제된 데이터를 조작하도록 실행될 수 있다.

[0046] [0048] 도 5는 작업 키에 기초하여 신규한 방식으로 데이터를 암호화 및 암호화해제하기 위한 프로세스(500)의 예시적 설계를 도시한다. 보안 서버(510)에서, 단-방향 키 유도 함수(KDF: key derivation function)(522)는, 디바이스(550)에 대해 허가된 소프트웨어와 관련될 수 있는 적어도 하나의 보안 파라미터(544) 및 하드웨어 비밀 키(542)에 기초하여 디바이스(550)에 대한 작업 키를 생성할 수 있다. 암호 엔진(530)은 작업 키로 데이터를 암호화하여 암호화된 데이터를 획득할 수 있고, 암호화된 데이터는 디바이스(550)에 전송될 수 있다.

[0047] [0049] 디바이스(550)에서, 키 유도 함수(522)는 디바이스(550)의 하드웨어 비밀 키(542) 및 적어도 하나의 보안 파라미터(544)에 기초하여 디바이스(550)에 대한 작업 키를 생성할 수 있다. 암호 엔진(570)은 보안 서버(510)로부터 암호화된 데이터를 수신할 수 있으며, 작업 키로 암호화된 데이터를 암호화해제하여 암호화해제된 데이터를 획득할 수 있다.

[0048] [0050] 보안 서버(510)에서, 하드웨어 비밀 키(542) 및/또는 보안 파라미터들(544)은 보안 서버(510) 내의 보안 저장소(541)에 저장될 수 있다. 키 유도 함수(522) 및 암호 엔진(530)은 하드웨어, 소프트웨어 및/또는 펌웨어로 구현될 수 있으며, 보안 서버(510) 내의 프로세서(521)에 의해 구현(예를 들어, 프로세서(521) 상에서 실행)될 수 있다.

[0049] [0051] 디바이스(550)에서, 하드웨어 비밀 키(542) 및/또는 보안 파라미터들(544)은 디바이스(550)의 보안 메모리(540)에 저장될 수 있다. 예를 들어, 보안 메모리(540)는 OTP 메모리를 포함할 수 있고, 하드웨어 비밀 키(542) 및/또는 보안 파라미터들(544)은 OTP 메모리의 퓨즈들을 블로우(blow)함으로써 저장될 수 있다. 키 유도 함수(522) 및 암호 엔진(570)은 하드웨어, 소프트웨어 및/또는 펌웨어로 구현될 수 있으며, 디바이스(550) 내의 프로세서(520)에 의해 구현(예를 들어, 그 상에서 실행)될 수 있다. 디바이스(550)는 도 1의 무선 디바이스(100)의 일 예시적 설계일 수 있다. 보안 메모리(540)는 도 1의 무선 디바이스(100) 내의 보안 메모리(140)에 대응할 수 있다. 프로세서(520)는 도 1의 무선 디바이스(100) 내의 프로세서(122 또는 124)에 대응할 수 있다.

[0050] [0052] 다양한 키 유도 함수들은 보안 서버(510) 및 디바이스(550)에서 키 유도 함수(522)에 대해 이용될 수 있다. 키 유도 함수는 SHA-1(보안 해쉬 알고리즘), SHA-2(이는 SHA-224, SHA-256, SHA-384 및 SHA-512를 포함함), MD-4(메시지 디지스트), MD-5 등과 같은 하나 또는 둘 이상의 암호법 해쉬 함수들을 이용할 수 있다. 보안 해쉬 알고리즘은, 입력 메시지와 출력 디지스트(이는 의사-랜덤 비트 스트링임) 사이의 함수가 역전할 수 없고(irreversible), 동일한 디지스트에의 2개의 입력 메시지들의 맵핑의 확률이 아주 작도록, 암호(cryptographic) 속성들을 갖는다. 키 유도 함수(522)는 공개적으로 입수가능한 NIST 800-108에서 설명되는 바와 같이 구현될 수 있다.

[0051] [0053] 도 2에 도시된 바와 같이, 보안 파라미터들(예를 들어, RoT(root-of-trust) 관련 보안 정보 및 보안 부트 관련 보안 정보)은 제조 프로세스의 일부로서 무선 디바이스의 보안 메모리에서 프로비저닝될 수 있다. 보안 파라미터들의 프로비저닝은 전형적으로, 하드웨어 비밀 키가 무선 디바이스 상에서 이미 프로비저닝된 이후 수행된다. 보안 파라미터들은 전형적으로 비밀이 아니며, 허가되지 않은 엔티티들(예를 들어, 제조 직원들)에 의해 프로비저닝될 수 있다.

[0052] [0054] 도 5에 도시된 바와 같이, 키 유도 함수는 디바이스 상에서 프로비저닝되는 하드웨어 비밀 키 및 적어도

하나의 보안 파라미터에 기초하여 작업 키를 생성하기 위해 이용될 수 있다. 보안 파라미터(들)는 디바이스에 대해 허가된 소프트웨어와 관련될 수 있다. 보안 파라미터(들)는 또한, 디바이스에 대한 시스템 보안 레벨 및/또는 특정 RoT(root-of-trust)를 결정할 수 있다. 작업 키는, 보안 파라미터(들)가 예를 들어, OEM에 의해 디바이스에 대해 프로비저닝된 이후 적절히 생성될 수 있다. 작업 키는 비밀 데이터를 보호하기 위해 OEM에 의해 이용될 수 있다. 허가되지 않은 소프트웨어는 디바이스에 대한 보안 파라미터들의 프로비저닝 이전에 디바이스에 악성으로 로딩될 수 있다. 그러나, 허가되지 않은 소프트웨어는 보안 파라미터들의 적절한 세트(right set) 없이 정확한(correct) 작업 키를 생성할 수 없을 것이다. 게다가, 부정확한 보안 파라미터들은 허가되지 않은 엔티티, 예를 들어, 신뢰성 없는 직원에 의해 디바이스로 로딩될 수 있다. 그러나, 정확한 작업 키는 보안 파라미터들의 적절한 세트 없이 생성되지 않을 것이고, 데이터는 여전히 보호될 것이다. 어느 경우든, 정확한 작업 키를 이용할 수 없는 소프트웨어는 디바이스 상에서 데이터를 적절히 암호화 또는 암호화해제할 수 없을 것이다.

[0053] [0055] 도 6은 보안을 제공하기 위한 프로세스(600)의 예시적 설계를 도시한다. 프로세스(600)는 디바이스, 또는 보안 서버, 또는 일부 다른 엔티티에 의해 수행될 수 있다. 작업 키는 (예를 들어, 키 유도 함수를 이용하여) 디바이스의 적어도 하나의 보안 파라미터 및 비밀 키(예를 들어, 하드웨어 비밀 키)에 기초하여 생성될 수 있다(블록(612)). 적어도 하나의 보안 파라미터는 디바이스에 대해 인증될 소프트웨어 및/또는 무선 디바이스에 대한 보안의 다른 양상들과 관련될 수 있다. 적어도 하나의 보안 기능은 작업 키에 기초하여 디바이스에 대해 수행될 수 있다(블록(614)). 작업 키는 적어도 하나의 보안 기능을 위해 소프트웨어에 의해 직접적으로 또는 간접적으로 이용될 수 있다. 적어도 하나의 보안 파라미터 및/또는 비밀 키는, 디바이스 상의, 예를 들어, OTP 엘리먼트들 내의, 보안 메모리에 저장될 수 있다.

[0054] [0056] 적어도 하나의 보안 파라미터는 디바이스에 대한 보안의 다양한 양상들을 제어할 수 있다. 하나의 설계에서, 적어도 하나의 보안 파라미터는 소프트웨어가(또는 어떤 소프트웨어가) 디바이스 상에서의 실행에 대해 허가되는지를 결정할 수 있다. 또 다른 설계에서, 적어도 하나의 보안 파라미터는 디바이스 상의 소프트웨어에 대해 허가된 적어도 하나의 동작 기능(또는 소프트웨어가 디바이스 상에서 어떻게 이용될 수 있는지)을 결정할 수 있다. 또 다른 설계에서, 적어도 하나의 보안 파라미터는 소프트웨어가 디바이스에 대해 허가되는지 여부를 결정하는데 이용되는 공개 키를 포함할 수 있다. 공개 키는, 예를 들어, 도 3a 및 3b에 도시된 바와 같이, 소프트웨어를 서명하는데 이용되는 개인 키에 대응할 수 있다. 적어도 하나의 보안 파라미터는 또한, 다른 타입들의 정보를 포함할 수 있다.

[0055] [0057] 하나의 설계에서, 비밀 키는 제 1 엔티티(예를 들어, IC 칩의 제조 동안, IC 칩 제조사)에 의해 디바이스로 로딩될 수 있다. 적어도 하나의 보안 파라미터는 제 1 엔티티와 상이할 수 있는 제 2 엔티티(예를 들어, OEM 또는 ODM 디바이스 제조)에 의해 디바이스로 로딩될 수 있다. 하나의 설계에서, 비밀 키 및 적어도 하나의 보안 파라미터는 상이한 시간들에서 디바이스로 로딩될 수 있다. 비밀 키 및 적어도 하나의 보안 파라미터는 상이한 다른 특성들을 가질 수 있다.

[0056] [0058] 블록(614)의 하나의 설계에서, 디바이스에 대한 데이터는 작업 키로 암호화 또는 서명될 수 있다. 블록(614)의 또 다른 설계에서, 디바이스에 대한 데이터는 작업 키로 암호화해제 또는 검증될 수 있다. 하나의 설계에서, 적어도 하나의 보안 기능은 소프트웨어의 제어 하에 수행될 수 있다.

[0057] [0059] 적어도 하나의 보안 기능은 소프트웨어를 인증하기 위해 보안 메커니즘(예를 들어, 보안 부트)의 활성화 이전에 소프트웨어에 의해 수행될 수 있다. 작업 키의 이용은 보안 메커니즘을 통해 소프트웨어를 인증하지 않고 소프트웨어가 디바이스 상에서 실행되게 할 수 있다.

[0058] [0060] 예시적 설계에서, 장치(예를 들어, ASIC, 무선 디바이스, 전자 디바이스 등)는 메모리 및 프로세서를 포함할 수 있다. 메모리(예를 들어, 도 1의 메모리(150))는 디바이스에 대한 소프트웨어를 저장할 수 있다. 프로세서(예를 들어, 도 1의 프로세서(122 또는 124)))는 메모리 (예를 들어, 하나 또는 둘 이상의 데이터 버스들을 통해)에 동작가능하게 커플링될 수 있다. 프로세서는 (i) 디바이스의 적어도 하나의 보안 파라미터 및 비밀 키에 기초하여 작업 키를 생성할 수 있고, (ii) 작업 키에 기초하여 디바이스에 대한 적어도 하나의 보안 기능(예를 들어, 암호화, 암호화해제, 시그니처, 검증 등)을 수행할 수 있다. 프로세서는 소프트웨어를 인증하기 위해 보안 메커니즘(예를 들어, 보안 부트)의 활성화 이전에 적어도 하나의 보안 기능을 수행할 수 있다. 적어도 하나의 보안 파라미터는 메모리에 저장된 소프트웨어의 인증과 관련될 수 있다. 작업 키는 적어도 하나의 보안 기능을 위해 소프트웨어에 의해 직접적으로 또는 간접적으로 이용될 수 있다. 비밀 키 및 적어도 하나의 보안 파라미터는 상이한 엔티티들에 의해 그리고/또는 상이한 시간들에서 디바이스로 로딩될 수 있다. 제 1 엔

티티는 비밀 키를 디바이스로 로딩할 수 있고, 제 2 엔티티는 적어도 하나의 보안 파라미터를 디바이스로 추후에 로딩할 수 있다. 제 1 엔티티는 IC 칩 제조일 수 있고, 제 2 엔티티는 OEM 또는 ODM일 수 있다. 대안적으로, 제 1 엔티티는 신뢰성 있는 직원일 수 있고, 제 2 엔티티는, 예를 들어, 동일한 제조 현장에서의 또는 상이한 위치들에서의 신뢰성 없는 직원일 수 있다. 장치는 비밀 키 및/또는 적어도 하나의 보안 파라미터를 저장하는 보안 메모리를 더 포함할 수 있다. 적어도 하나의 보안 파라미터는 또한, 적어도 하나의 보안 파라미터의 무결성이 메모리에 의해 보호되는 한, 장치 상의 불안전한 메모리에 저장될 수 있다.

[0059] [0061] 본원에 개시된 보안 키 생성 기법들은 다양한 이점들을 제공할 수 있다. 기법들은 허가되지 않은 소프트웨어가 보안 부트의 활성화 이전에 제조 시 취약한 시간 기간 동안 하드웨어 비밀 키를 이용하는 것 또는 데이터를 조작하는 것을 방지할 수 있다. 이것은 OEM/ODM가 제조 현장을 안전하게 보호하기 위해 다양한 프로세스들을 구현하여야 하는 것을 면하게 할 수 있다. 본원에 개시된 기법들에 의해 제공된 다른 이점들이 존재할 수 있다.

[0060] [0062] 당업자들은 정보 및 신호들이 다양한 상이한 기술들 및 기법들 중 임의의 것을 이용하여 표현될 수 있다는 것을 이해할 것이다. 예를 들어, 상기 설명의 전체에 걸쳐 참조될 수 있는 데이터, 명령들, 커맨드들, 정보, 신호들, 비트들, 심볼들 및 칩들은 전압들, 전류들, 전자기파들, 자기장들 또는 자기 입자들, 광 필드들 또는 광입자들 또는 이들의 임의의 결합으로 표현될 수 있다.

[0061] [0063] 당업자들은 본원에서의 개시와 관련하여 설명된 다양한 예시적 논리 블록들, 모듈들, 회로들 및 알고리즘 단계들이 전자 하드웨어, 컴퓨터 소프트웨어 또는 이 둘의 결합들로서 구현될 수 있다는 것을 추가로 인식할 것이다. 하드웨어 및 소프트웨어의 이러한 상호교환가능성을 명백하게 예시하기 위해, 다양한 예시적 컴포넌트들, 블록들, 모듈들, 회로들 및 단계들이 일반적으로 그들의 기능에 관하여 위에서 설명되었다. 이러한 기능이 하드웨어로서 구현되는지 또는 소프트웨어로서 구현되는지는 전체 시스템 상에 부과되는 설계 제약들 및 특정 애플리케이션에 의존한다. 당업자들은 각각의 특정 애플리케이션에 대해 다양한 방식들로 설명된 기능을 구현할 수 있지만, 이러한 구현 결정들은 본 개시의 범위를 벗어나게 하는 것으로 해석되어서는 안 된다.

[0062] [0064] 본원에서의 개시와 관련하여 설명된 다양한 예시적 논리 블록들, 모듈들 및 회로들은 범용 프로세서, DSP(digital signal processor), ASIC(application specific integrated circuit), FPGA(field programmable gate array) 또는 다른 프로그래머블 로직 디바이스, 이산 게이트 또는 트랜지스터 로직, 이산 하드웨어 컴포넌트들, 또는 본원에 설명된 기능들을 수행하도록 설계되는 이들의 임의의 결합으로 구현 또는 수행될 수 있다. 범용 프로세서는 마이크로프로세서일 수 있지만, 대안적으로, 프로세서는 임의의 종래의 프로세서, 제어기, 마이크로제어기 또는 상태 머신일 수 있다. 또한, 프로세서는 컴퓨팅 디바이스들의 결합 예를 들어, DSP 및 마이크로프로세서의 결합, 복수의 마이크로프로세서들, DSP 코어와 결합된 하나 또는 둘 이상의 마이크로프로세서들, 또는 임의의 다른 이러한 구성으로서 구현될 수 있다.

[0063] [0065] 본원에서의 개시와 관련하여 설명된 알고리즘 또는 방법의 단계들은 직접적으로 하드웨어로, 프로세서에 의해 실행되는 소프트웨어 모듈로, 또는 이 둘의 결합으로 구현될 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. 예시적 저장 매체는, 프로세서가 저장 매체로부터 정보를 판독하고, 저장 매체에 정보를 기록할 수 있도록, 프로세서에 커플링된다. 대안적으로, 저장 매체는 프로세서에 통합될 수 있다. 프로세서 및 저장 매체는 ASIC에 상주할 수 있다. ASIC는 사용자 단말에 상주할 수 있다. 대안적으로, 프로세서 및 저장 매체는 사용자 단말에서 별개의 컴포넌트들로서 상주할 수 있다.

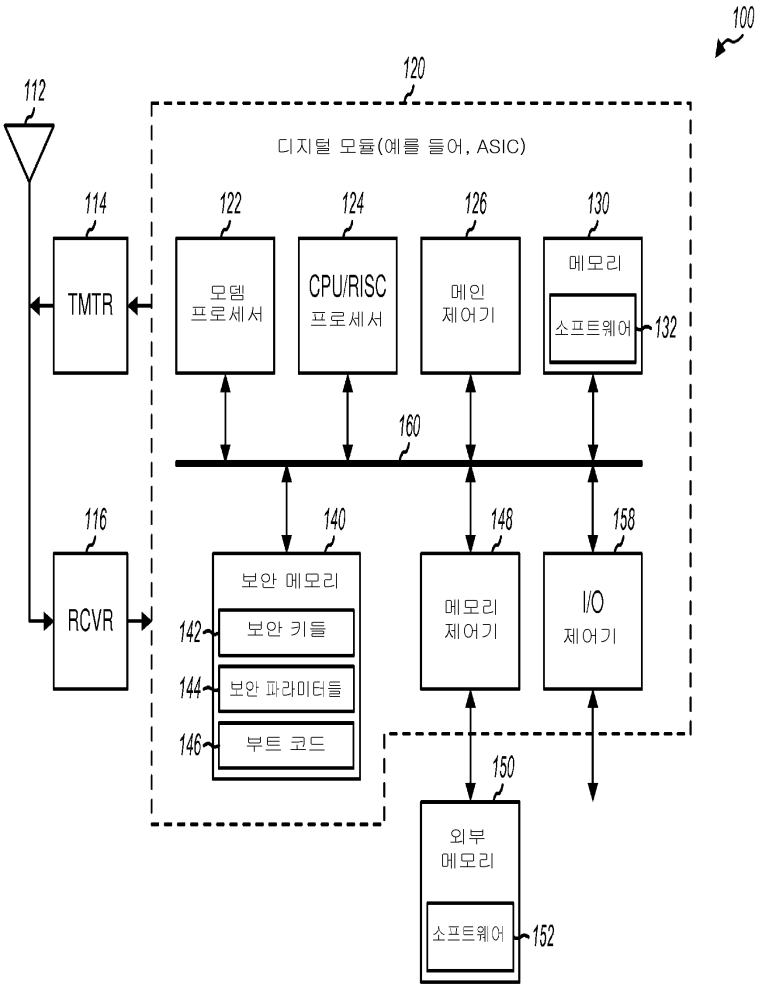
[0064] [0066] 하나 또는 둘 이상의 예시적 설계들에서, 설명된 기능들은 하드웨어, 소프트웨어, 펌웨어 또는 이들의 임의의 결합으로 구현될 수 있다. 소프트웨어로 구현되는 경우, 기능들은 컴퓨터 판독가능한 매체 상에 하나 또는 둘 이상의 명령들 또는 코드로서 저장되거나 이를 통해 송신될 수 있다. 컴퓨터 판독가능한 매체들은 하나의 장소에서 다른 장소로 컴퓨터 프로그램의 이전을 가능하게 하는 임의의 매체를 포함하는 통신 매체들 및 컴퓨터 저장 매체들 둘 모두를 포함한다. 저장 매체들은 범용 또는 특수 목적의 컴퓨터에 의해 액세스될 수 있는 임의의 이용가능한 매체들일 수 있다. 제한이 아닌 예로서, 이러한 컴퓨터 판독가능한 매체들은 RAM, ROM, EEPROM, CD-ROM 또는 다른 광학 디스크 스토리지, 자기 디스크 스토리지 또는 다른 자기 저장 디바이스들, 또는 원하는 프로그램 코드 수단을 명령들 또는 데이터 구조들의 형태로 전달 또는 저장하기 위해 이용될 수 있고 범용 또는 특수 목적의 컴퓨터 또는 범용 또는 특수 목적의 프로세서에 의해 액세스될 수 있는 임의의 다른 매체를 포함할 수 있다. 또한, 임의의 연결은 컴퓨터 판독가능한 매체로 적절히 지칭된다. 예를 들어, 소프트웨어

가 웹사이트, 서버, 또는 다른 원격 소스로부터 동축 케이블, 광섬유 케이블, 꼬임 쌍선, DSL(digital subscriber line), 또는 (적외선, 라디오 및 마이크로파와 같은) 무선 기술들을 이용하여 송신되는 경우, 동축 케이블, 광섬유 케이블, 꼬임 쌍선, DSL, 또는 (적외선, 라디오 및 마이크로파와 같은) 무선 기술들이 매체의 정의 내에 포함된다. 본원에서 이용되는 바와 같은 디스크(disk) 및 디스크(disc)는 CD(compact disc), 레이저 디스크(disc), 광 디스크(disc), DVD(digital versatile disc), 플로피 디스크(disk) 및 블루-레이 디스크(disc)를 포함하며, 여기서 디스크(disk)들은 통상적으로 데이터를 자기적으로 재생하는 반면, 디스크(disc)들은 광학적으로 레이저들을 이용하여 데이터를 재생한다. 위의 것들의 결합들이 또한, 컴퓨터 판독가능한 매체들의 범위 내에 포함되어야 한다.

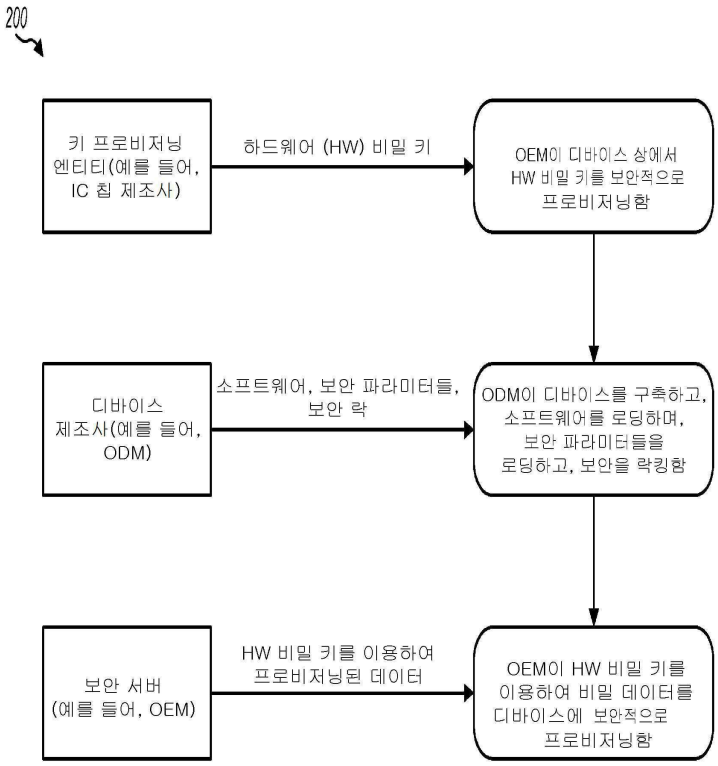
[0065] [0067] 본 개시의 이전의 설명은 임의의 당업자가 본 개시를 실시하거나 또는 이용할 수 있도록 제공된다. 본 개시에 대한 다양한 변경들은 당업자들에게 쉽게 명백할 것이고, 본원에서 정의된 일반적 원리들은 본 개시의 범위를 벗어나지 않으면서 다른 변형들에 적용될 수 있다. 따라서, 본 개시는 본원에서 설명된 예들 및 설계들에 제한되는 것으로 의도된 것이 아니라, 본원에 개시된 원리들 및 신규한 특징들과 일치하는 가장 넓은 범위를 따를 것이다.

## 도면

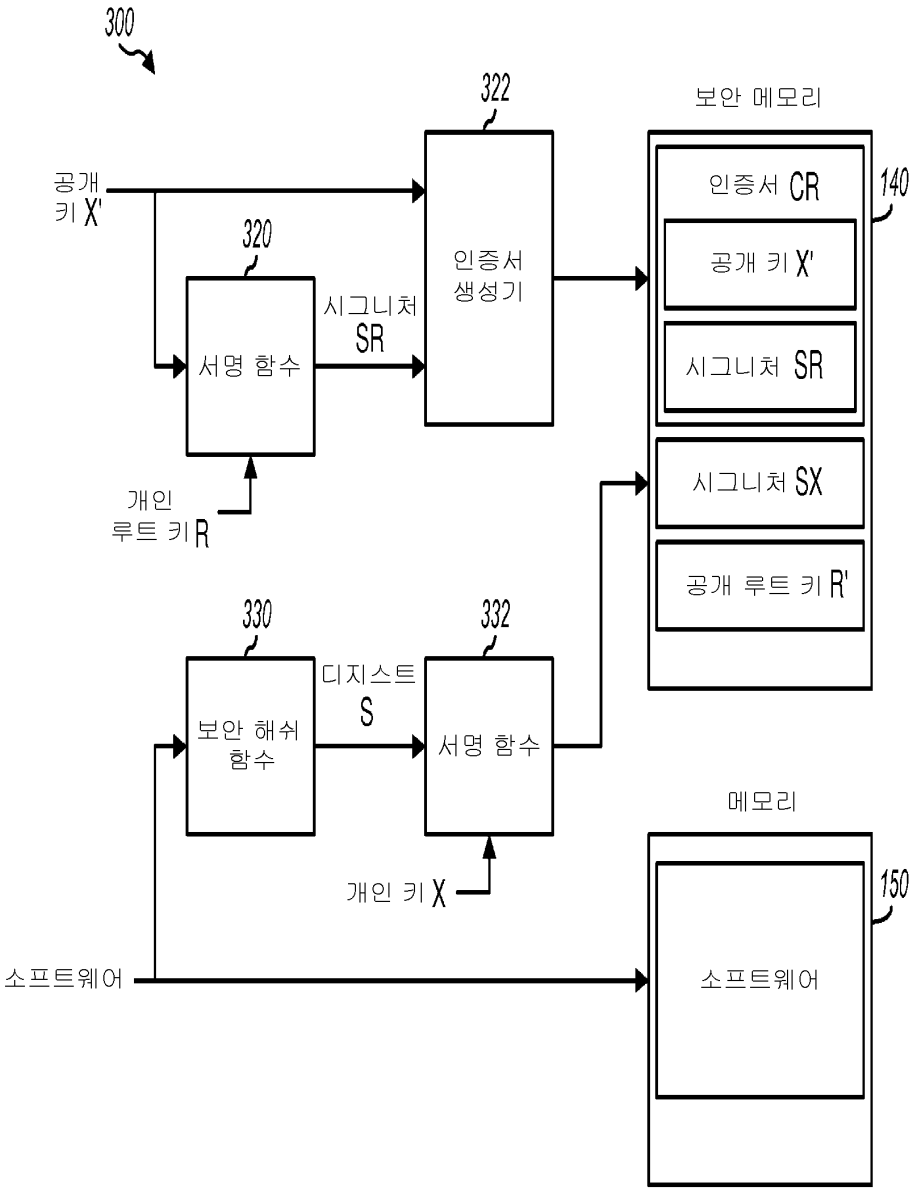
### 도면1



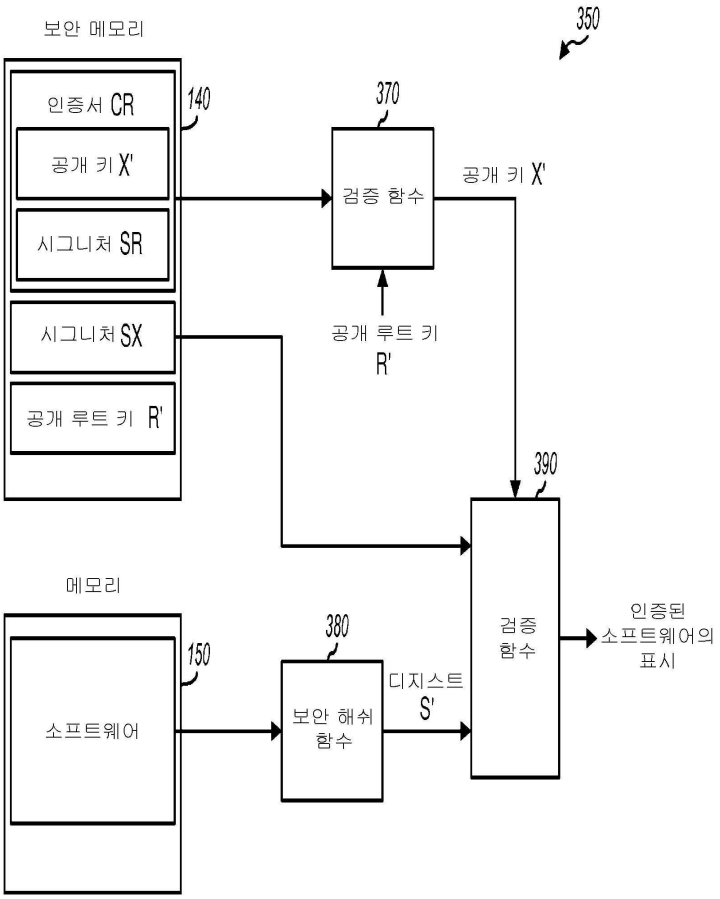
도면2


200
키 프로비저닝 엔티티(예를 들어, IC 칩 제조사)
하드웨어 (HW) 비밀 키
OEM이 디바이스 상에서 HW 비밀 키를 보안적으로 프로비저닝함
디바이스 제조사(예를 들어, ODM)
소프트웨어, 보안 파라미터들, 보안 락
ODM이 디바이스를 구축하고, 소프트웨어를 로딩하며, 보안 파라미터들을 로딩하고, 보안을 락킹함
보안 서버 (예를 들어, OEM)
HW 비밀 키를 이용하여 프로비저닝된 데이터
OEM이 HW 비밀 키를 이용하여 비밀 데이터를 디바이스에 보안적으로 프로비저닝함

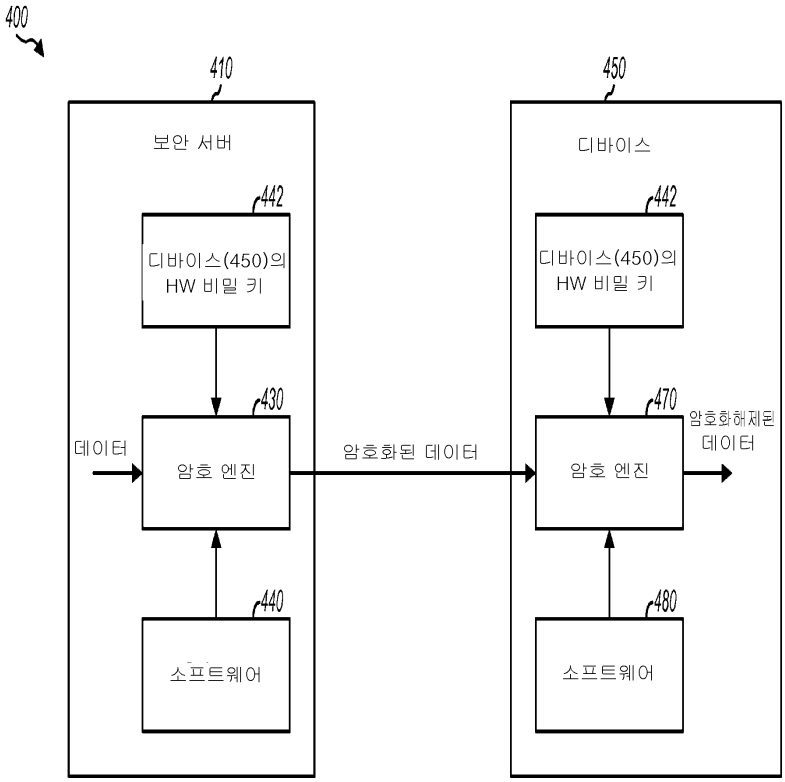
도면3a


300
322
보안 메모리
공개 키 X'
320
인증서 생성기
인증서 CR
140
공개 키 X'
시그니처 SR
서명 함수
시그니처 SR
시그니처 SX
개인 루트 키 R
공개 루트 키 R'
330
332
디지스트 S
보안 해쉬 함수
서명 함수
메모리
개인 키 X
150
소프트웨어
소프트웨어

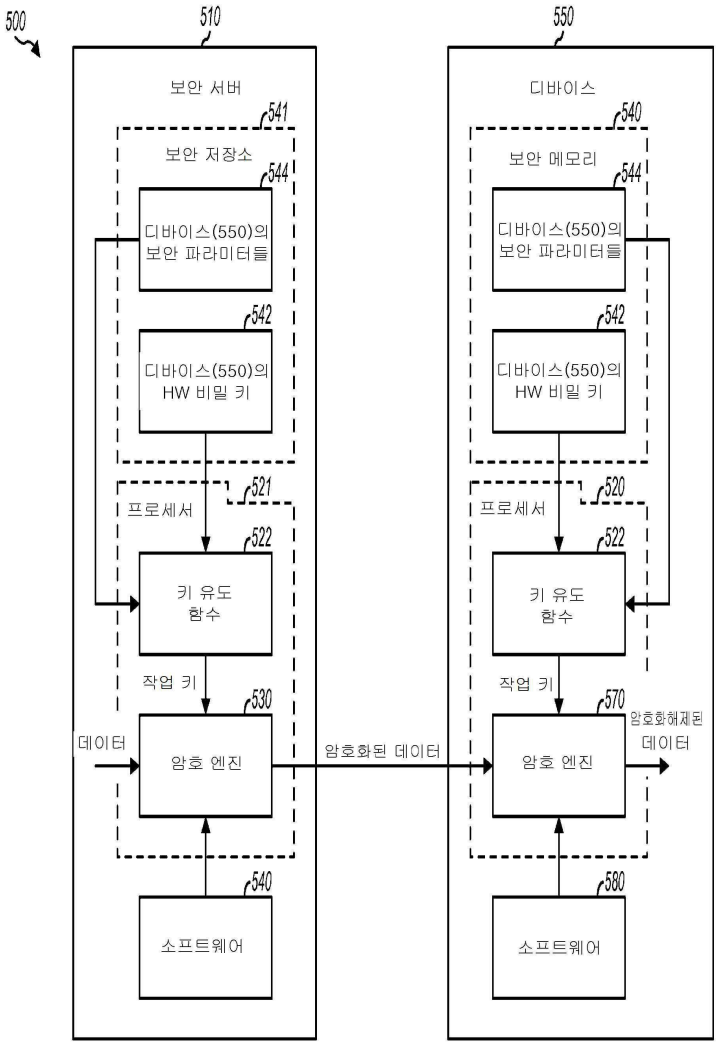
도면3b


보안 메모리
350
인증서 CR
공개 키 X'
시그니처 SR
시그니처 SX
공개 루트 키 R'
140
370
검증 함수
공개 키 X'
공개 루트 키 R'
390
메모리
150
소프트웨어
380
보안 해쉬 함수
디지스트 S'
검증 함수
인증된 소프트웨어의 표시

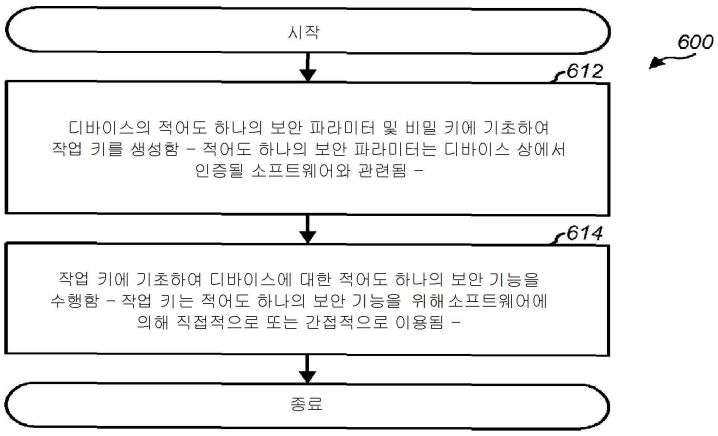
도면4


400
410
보안 서버
442
디바이스(450)의
HW 비밀 키
430
데이터
암호 엔진
440
소프트웨어
암호화된 데이터
450
디바이스
442
디바이스(450)의
HW 비밀 키
470
암호화해제된
데이터
암호 엔진
480
소프트웨어

도면5


500
510
보안 서버
541
보안 저장소
544
디바이스(550)의 보안 파라미터들
542
디바이스(550)의 HW 비밀 키
521
프로세서
522
키 유도 함수
작업 키
530
데이터
암호 엔진
540
소프트웨어
암호화된 데이터
550
디바이스
540
보안 메모리
544
디바이스(550)의 보안 파라미터들
542
디바이스(550)의 HW 비밀 키
520
프로세서
522
키 유도 함수
작업 키
570
암호 엔진
암호화해제된 데이터
580
소프트웨어

도면6


시작
600
612
디바이스의 적어도 하나의 보안 파라미터 및 비밀 키에 기초하여 작업 키를 생성함 - 적어도 하나의 보안 파라미터는 디바이스 상에서 인증될 소프트웨어와 관련됨 -
614
작업 키에 기초하여 디바이스에 대한 적어도 하나의 보안 기능을 수행함 - 작업 키는 적어도 하나의 보안 기능을 위해 소프트웨어에 의해 직접적으로 또는 간접적으로 이용됨 -
종료