(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2016-0140666
(43) 공개일자 2016년12월07일

(51) 국제특허분류(Int. Cl.)
G06F 21/33 (2013.01) *G01R 31/317* (2006.01)
H04L 29/06 (2006.01) *H04L 9/30* (2006.01)
H04L 9/32 (2006.01)
(52) CPC특허분류
G06F 21/335 (2013.01)
G01R 31/31705 (2013.01)
(21) 출원번호 10-2016-7026928
(22) 출원일자(국제) 2015년03월31일
심사청구일자 없음
(85) 번역문제출일자 2016년09월28일
(86) 국제출원번호 PCT/US2015/023518
(87) 국제공개번호 WO 2015/153562
국제공개일자 2015년10월08일
(30) 우선권주장
14/245,661 2014년04월04일 미국(US)

(71) 출원인
퀄컴 인코포레이티드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
맥클레인, 이반 휴
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(74) 대리인
특허법인 남앤드남

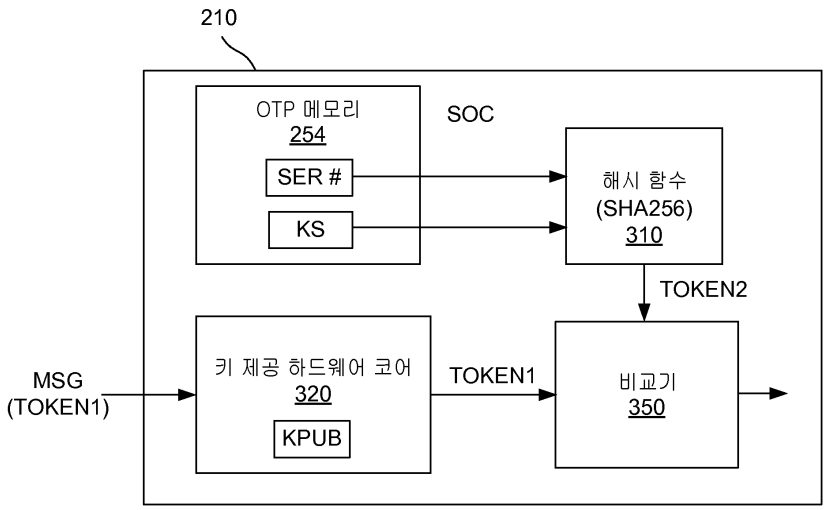
전체 청구항 수 : 총 30 항

(54) 발명의 명칭 **단일 칩 시스템 디바이스에서 디세이블된 디버그 성능을 재-인에이블하기 위한 방법 및 원격국**

(57) 요 약

단일 칩 시스템(SoC) 디바이스와 같은 집적 회로에서 디세이블된 디버그 성능이 안전하게 재-인에이블될 수 있다. 방법에서, 집적 회로가 디버그 재-인에이블 메시지를 수신한다. 디버그 재-인에이블 메시지는 개인키에 의해 서명된 디버그 재-인에이블 토큰을 포함한다. 디버그 재-인에이블 토큰은 집적 회로의 일련번호 및 대칭키의 제 1 사본을 기초로 한다. 디버그 재-인에이블 토큰은 개인키에 대응하는 공개키를 사용하여 인증된다. 집적 회로의 일련번호를 사용하여 그리고 집적 회로의 1회 프로그램 가능(OTP) 메모리에 저장된 대칭키의 제 2 사본을 사용하여 비교 토큰이 생성된다. 집적 회로는 디버그 재-인에이블 토큰과 비교 토큰을 비교한다. 디버그 재-인에이블 토큰이 비교 토큰과 일치한다면, 집적 회로에서 디세이블된 디버그 성능이 재-인에이블된다.

대 표 도 - 도3



(52) CPC특허분류
G01R 31/31719 (2013.01)
H04L 63/0807 (2013.01)
H04L 9/30 (2013.01)
H04L 9/3263 (2013.01)

명 세 서

청구범위

청구항 1

집적 회로에서 디세이블(disable)된 디버그 성능을 재-인에이블(re-enable)하기 위한 방법으로서,

상기 집적 회로에 의해 제 1 관계자로부터 디버그 재-인에이블 메시지를 수신하는 단계 - 상기 디버그 재-인에이블 메시지는 상기 제 1 관계자의 개인키에 의해 서명된 디버그 재-인에이블 토큰을 포함하고,

상기 디버그 재-인에이블 토큰은 상기 집적 회로의 고유 식별자 및 제 2 관계자의 대칭키의 제 1 사본을 기초로 하며,

상기 대칭키는 상기 제 1 관계자에게 이용 가능하지 않음 -;

상기 개인키에 대응하는 공개키를 사용하여 상기 디버그 재-인에이블 토큰을 인증하는 단계;

상기 고유 식별자를 사용하여 그리고 상기 집적 회로에 안전하게 저장된 상기 대칭키의 제 2 사본을 사용하여 비교 토큰을 생성하는 단계;

상기 집적 회로에 의해 상기 디버그 재-인에이블 토큰과 상기 비교 토큰을 비교하는 단계; 및

상기 디버그 재-인에이블 토큰이 상기 비교 토큰과 일치한다면, 상기 집적 회로에서 상기 디세이블된 디버그 성능을 재-인에이블하는 단계를 포함하는,

집적 회로에서 디세이블된 디버그 성능을 재-인에이블하기 위한 방법.

청구항 2

제 1 항에 있어서,

상기 집적 회로는 단일 칩 시스템(SoC: system-on-a chip) 디바이스인,

집적 회로에서 디세이블된 디버그 성능을 재-인에이블하기 위한 방법.

청구항 3

제 1 항에 있어서,

상기 디버그 재-인에이블 메시지는 상기 제 1 관계자로부터 직접 수신되는,

집적 회로에서 디세이블된 디버그 성능을 재-인에이블하기 위한 방법.

청구항 4

제 3 항에 있어서,

상기 대칭키의 제 1 사본은 상기 제 2 관계자에 저장되는,

집적 회로에서 디세이블된 디버그 성능을 재-인에이블하기 위한 방법.

청구항 5

제 1 항에 있어서,

상기 제 1 관계자의 개인키는 상기 제 2 관계자에게 이용 가능하지 않은,

집적 회로에서 디세이블된 디버그 성능을 재-인에이블하기 위한 방법.

청구항 6

제 1 항에 있어서,

상기 고유 식별자는 상기 집적 회로의 일련번호인,

집적 회로에서 디세이블된 디버그 성능을 재-인에이블하기 위한 방법.

청구항 7

제 6 항에 있어서,

상기 비교 토큰은 상기 일련번호 및 상기 대칭키의 제 2 사본을 입력들로서 사용하는 단방향 암호화 함수를 기초로 생성되는,

집적 회로에서 디세이블된 디버그 성능을 재-인에이블하기 위한 방법.

청구항 8

제 1 항에 있어서,

상기 대칭키는 상기 집적 회로의 1회 프로그램 가능(OTP: one-time-programmable) 메모리에 안전하게 저장되는,

집적 회로에서 디세이블된 디버그 성능을 재-인에이블하기 위한 방법.

청구항 9

원격국으로서,

제 1 관계자로부터 디버그 재-인에이블 메시지를 수신하기 위한 수단 - 상기 디버그 재-인에이블 메시지는 상기 제 1 관계자의 개인키에 의해 서명된 디버그 재-인에이블 토큰을 포함하고, 상기 디버그 재-인에이블 토큰은 집적 회로의 고유 식별자 및 제 2 관계자의 대칭키의 제 1 사본을 기초로 하며, 상기 대칭키는 상기 제 1 관계자에게 이용 가능하지 않음 -;

상기 개인키에 대응하는 공개키를 사용하여 상기 디버그 재-인에이블 토큰을 인증하기 위한 수단;

상기 고유 식별자를 사용하여 그리고 상기 집적 회로에 안전하게 저장된 상기 대칭키의 제 2 사본을 사용하여 비교 토큰을 생성하기 위한 수단;

상기 디버그 재-인에이블 토큰과 상기 비교 토큰을 비교하기 위한 수단; 및

상기 디버그 재-인에이블 토큰이 상기 비교 토큰과 일치한다면, 상기 집적 회로에서 디세이블된 디버그 성능을 재-인에이블하기 위한 수단을 포함하는,

원격국.

청구항 10

제 9 항에 있어서,

상기 집적 회로는 단일 칩 시스템(SoC) 디바이스인,

원격국.

청구항 11

제 9 항에 있어서,

상기 디버그 재-인에이블 메시지는 상기 제 1 관계자로부터 직접 수신되고,

상기 개인 키는 상기 제 1 관계자에 대한 것인,

원격국.

청구항 12

제 11 항에 있어서,

상기 대칭키의 제 1 사본은 상기 제 2 관계자에 저장되는,

원격국.

청구항 13

제 9 항에 있어서,

상기 제 1 관계자의 개인키는 상기 제 2 관계자에게 이용 가능하지 않은,

원격국.

청구항 14

제 9 항에 있어서,

상기 고유 식별자는 상기 집적 회로의 일련번호인,

원격국.

청구항 15

제 14 항에 있어서,

상기 비교 토큰은 상기 일련번호 및 상기 대칭키의 제 2 사본을 입력들로서 사용하는 단방향 암호화 함수를 기초로 생성되는,

원격국.

청구항 16

제 9 항에 있어서,

상기 대칭키는 상기 집적 회로의 1회 프로그램 가능(OTP) 메모리에 안전하게 저장되는,

원격국.

청구항 17

원격국으로서,

프로세서를 포함하며,

상기 프로세서는,

제 1 관계자로부터 디버그 재-인에이블 메시지를 수신하고 - 상기 디버그 재-인에이블 메시지는 상기 제 1 관계자의 개인키에 의해 서명된 디버그 재-인에이블 토큰을 포함하고, 상기 디버그 재-인에이블 토큰은 집적 회로의 고유 식별자 및 제 2 관계자의 대칭키의 제 1 사본을 기초로 하며, 상기 대칭키는 상기 제 1 관계자에게 이용 가능하지 않음 -;

상기 개인키에 대응하는 공개키를 사용하여 상기 디버그 재-인에이블 토큰을 인증하고;

상기 고유 식별자를 사용하여 그리고 상기 집적 회로에 안전하게 저장된 상기 대칭키의 제 2 사본을 사용하여 비교 토큰을 생성하고;

상기 디버그 재-인에이블 토큰과 상기 비교 토큰을 비교하고; 그리고

상기 디버그 재-인에이블 토큰이 상기 비교 토큰과 일치한다면, 상기 집적 회로에서 디세이블된 디버그 성능을 재-인에이블하도록 구성되는,

원격국.

청구항 18

제 17 항에 있어서,

상기 집적 회로는 단일 칩 시스템(SoC) 디바이스인,

원격국.

청구항 19

제 17 항에 있어서,

상기 디버그 재-인에이블 메시지는 상기 제 1 관계자로부터 직접 수신되는,

원격국.

청구항 20

제 19 항에 있어서,

상기 대칭키의 제 1 사본은 상기 제 2 관계자에 저장되는,

원격국.

청구항 21

제 17 항에 있어서,

상기 제 1 관계자의 개인키는 상기 제 2 관계자에게 이용 가능하지 않은,

원격국.

청구항 22

제 17 항에 있어서,

상기 고유 식별자는 상기 집적 회로의 일련번호인,

원격국.

청구항 23

제 22 항에 있어서,

상기 비교 토큰은 상기 일련번호 및 상기 대칭키의 제 2 사본을 입력들로서 사용하는 단방향 암호화 함수를 기초로 생성되는,

원격국.

청구항 24

제 18 항에 있어서,

상기 대칭키는 상기 집적 회로의 1회 프로그램 가능(OTP) 메모리에 안전하게 저장되는,

원격국.

청구항 25

집적 회로로서,

제 1 관계자로부터 디버그 재-인에이블 메시지를 수신하기 위한 수단 - 상기 디버그 재-인에이블 메시지는 상기 제 1 관계자의 개인키에 의해 서명된 디버그 재-인에이블 토큰을 포함하고, 상기 디버그 재-인에이블 토큰은 상기 집적 회로의 고유 식별자 및 제 2 관계자의 대칭키의 제 1 사본을 기초로 하며, 상기 대칭키는 상기 제 1 관계자에게 이용 가능하지 않음 -;

상기 개인키에 대응하는 공개키를 사용하여 상기 디버그 재-인에이블 토큰을 인증하기 위한 수단;

상기 고유 식별자를 사용하여 그리고 상기 집적 회로에 안전하게 저장된 상기 대칭키의 제 2 사본을 사용하여 비교 토큰을 생성하기 위한 수단;

상기 디버그 재-인에이블 토큰과 상기 비교 토큰을 비교하기 위한 수단; 및

상기 디버그 재-인에이블 토큰이 상기 비교 토큰과 일치한다면, 상기 집적 회로에서 디세이블된 디버그 성능을 재-인에이블하기 위한 수단을 포함하는,

집적 회로.

청구항 26

제 25 항에 있어서,

상기 집적 회로는 단일 칩 시스템(SoC) 디바이스인,

집적 회로.

청구항 27

제 25 항에 있어서,

상기 디버그 재-인에이블 메시지는 상기 제 1 관계자로부터 직접 수신되고,

상기 대칭키의 제 1 사본은 상기 제 2 관계자에 저장되는,

집적 회로.

청구항 28

제 25 항에 있어서,

상기 고유 식별자는 상기 집적 회로의 일련번호인,

집적 회로.

청구항 29

제 28 항에 있어서,

상기 비교 토큰은 상기 일련번호 및 상기 대칭키의 제 2 사본을 입력들로서 사용하는 단방향 암호화 함수를 기초로 생성되는,

집적 회로.

청구항 30

제 25 항에 있어서,

상기 대칭키는 상기 집적 회로의 1회 프로그램 가능(OTP) 메모리에 안전하게 저장되는,

집적 회로.

발명의 설명

기 술 분 야

[0001] [0001] 본 출원은 미국 특허 및 상표청에 2014년 4월 4일자 출원된 미국 비-가특허출원 제14/245,661호에 대한 우선권 및 이익을 주장하며, 이 특허출원의 전체 내용이 인용에 의해 본 명세서에 포함된다.

[0002] [0002] 본 발명은 일반적으로 단일 칩 시스템(SoC: system-on-a-chip) 디바이스에서의 디세이블(disable)된 디버그 성능 재-인에이블(re-enable)에 관한 것이다.

배 경 기 술

[0003] [0003] 단일 칩 시스템(SoC) 디바이스에서의 디버그 재-인에이블은 보안 민감도들을 야기한다. SoC 디바이스를 그 제품들에 포함시키는 주문자 상표 부착 생산자(OEM: original equipment manufacturer)는 자신의 보안 방식이 절충되길 원하지 않으며, SoC 디바이스의 생산자/공급자는 가능한 생산 또는 다른 결함을 기초로 반납된 디바이스를 디버그하도록 허용되어야 한다. 일부 OEM들은 보안에 대해 걱정하지 않을 수도 있고, 이들의 부품에

대한 추가 보안 노력을 필요로 하지 않으면서 단지 작업할 것들만을 원할 수도 있다.

[0004] [0004] 따라서 SoC 디바이스에서 디세이블된 디버그 성능을 효율적인 방식으로 재-인에이블하기 위한 기술에 대한 필요성이 존재한다.

발명의 내용

[0005] [0005] 본 발명의 한 양상은 집적 회로에서 디세이블된 디버그 성능을 재-인에이블하기 위한 방법에 있을 수도 있다. 이 방법에서, 집적 회로가 디버그 재-인에이블 메시지를 수신한다. 디버그 재-인에이블 메시지는 개인키에 의해 서명된 디버그 재-인에이블 토큰을 포함한다. 디버그 재-인에이블 토큰은 집적 회로의 고유 식별자 및 대칭키의 제 1 사본을 사용하여 생성된다. 디버그 재-인에이블 토큰은 개인키에 대응하는 공개키를 사용하여 인증된다. 고유 식별자를 사용하여 그리고 집적 회로에 안전하게 저장된 대칭키의 제 2 사본을 사용하여 비교 토큰이 생성된다. 집적 회로는 디버그 재-인에이블 토큰과 비교 토큰을 비교한다. 디버그 재-인에이블 토큰이 비교 토큰과 일치한다면, 집적 회로에서 디세이블된 디버그 성능이 재-인에이블된다.

[0006] [0006] 본 발명의 보다 상세한 양상들에서, 집적 회로는 단일 칩 시스템(SoC) 디바이스일 수도 있다. 디버그 재-인에이블 메시지는 제 1 관계자로부터 수신될 수 있고, 개인키는 제 1 관계자에 대한 것일 수도 있다. 대칭키의 제 1 사본은 제 2 관계자에 저장될 수도 있다. 제 1 관계자의 개인키는 제 2 관계자에게 이용 가능하지 않고, 대칭키는 제 1 관계자에게 이용 가능하지 않다. 고유 식별자는 집적 회로의 일련번호일 수도 있다. 비교 토큰은 일련번호 및 대칭키의 제 2 사본을 입력들로서 사용하는 단방향 암호화 함수를 기초로 생성될 수도 있다. 대칭키는 집적 회로의 1회 프로그램 가능(OTP: one-time-programmable) 메모리에 안전하게 저장될 수 있다.

[0007] [0007] 본 발명의 다른 양상은 원격국에 있을 수 있는데, 이는: 디버그 재-인에이블 메시지를 수신하기 위한 수단 – 메시지는 개인키에 의해 서명된 디버그 재-인에이블 토큰을 포함하고, 디버그 재-인에이블 토큰은 집적 회로의 고유 식별자 및 대칭키의 제 1 사본을 기초로 함 –; 개인키에 대응하는 공개키를 사용하여 디버그 재-인에이블 토큰을 인증하기 위한 수단; 고유 식별자를 사용하여 그리고 집적 회로에 안전하게 저장된 대칭키의 제 2 사본을 사용하여 비교 토큰을 생성하기 위한 수단; 디버그 재-인에이블 토큰과 비교 토큰을 비교하기 위한 수단; 및 디버그 재-인에이블 토큰이 비교 토큰과 일치한다면, 집적 회로에서 디세이블된 디버그 성능을 재-인에이블하기 위한 수단을 포함한다.

[0008] [0008] 본 발명의 다른 양상은 원격국에 있을 수 있는데, 이는: 디버그 재-인에이블 메시지를 수신하고 – 메시지는 개인키에 의해 서명된 디버그 재-인에이블 토큰을 포함하고, 디버그 재-인에이블 토큰은 집적 회로의 고유 식별자 및 대칭키의 제 1 사본을 기초로 함 –; 개인키에 대응하는 공개키를 사용하여 디버그 재-인에이블 토큰을 인증하고; 고유 식별자를 사용하여 그리고 집적 회로에 안전하게 저장된 대칭키의 제 2 사본을 사용하여 비교 토큰을 생성하고; 디버그 재-인에이블 토큰과 비교 토큰을 비교하고; 그리고 디버그 재-인에이블 토큰이 비교 토큰과 일치한다면, 집적 회로에서 디세이블된 디버그 성능을 재-인에이블하도록 구성된 프로세서를 포함한다.

[0009] [0009] 본 발명의 다른 양상은 집적 회로에 있을 수 있는데, 이는: 디버그 재-인에이블 메시지를 수신하기 위한 수단 – 메시지는 개인키에 의해 서명된 디버그 재-인에이블 토큰을 포함하고, 디버그 재-인에이블 토큰은 집적 회로의 고유 식별자 및 대칭키의 제 1 사본을 기초로 함 –; 개인키에 대응하는 공개키를 사용하여 디버그 재-인에이블 토큰을 인증하기 위한 수단; 고유 식별자를 사용하여 그리고 집적 회로에 안전하게 저장된 대칭키의 제 2 사본을 사용하여 비교 토큰을 생성하기 위한 수단; 디버그 재-인에이블 토큰과 비교 토큰을 비교하기 위한 수단; 및 디버그 재-인에이블 토큰이 비교 토큰과 일치한다면, 집적 회로에서 디세이블된 디버그 성능을 재-인에이블하기 위한 수단을 포함한다.

도면의 간단한 설명

[0010] [0010] 도 1은 무선 통신 시스템의 일례의 블록도이다.

[0011] [0011] 도 2는 본 발명에 따라, 단일 칩 시스템(SoC) 디바이스와 같은 집적 회로에서 디세이블된 디버그 성능을 재-인에이블하기 위한 방법의 블록도이다.

[0012] [0012] 도 3은 SoC 디바이스의 블록도이다.

[0013] [0013] 도 4는 프로세서 및 메모리를 포함하는 컴퓨터의 블록도이다.

[0014] 도 5는 개인키를 사용하여 토큰에 대한 서명을 생성하기 위한 방법의 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0011] [0015] 본 명세서에서 "예시적인"이라는 단어는 "일례, 실례 또는 예시로서의 역할"을 의미하는데 사용된다. 본 명세서에서 "예시적인" 것으로서 설명된 어떠한 실시예도 반드시 다른 실시예들에 비해 선호되거나 유리한 것으로 해석되는 것은 아니다.

[0012] [0016] 도 2와 도 3을 참조하면, 본 발명의 한 양상은 단일 칩 시스템(SoC) 디바이스(210)와 같은 집적 회로에서 디세이블된 디버그 성능을 재-인에이블하기 위한 방법(200)에 있을 수도 있다. 이 방법에서, 집적 회로가 디버그 재-인에이블 메시지(MSG)를 수신한다(단계(230)). 디버그 재-인에이블 메시지는 개인키(KPRI)에 의해 서명된 디버그 재-인에이블 토큰(TOKEN1)을 포함한다. 디버그 재-인에이블 토큰은 집적 회로의 고유 식별자 및 대칭키(KS)의 제 1 사본을 기초로 할 수도 있다. 디버그 재-인에이블 토큰은 개인키에 대응하는 공개키(KPUB)를 사용하여 인증된다(단계(250)). 고유 식별자를 사용하여 그리고 집적 회로에 안전하게 저장된 대칭키의 제 2 사본을 사용하여 비교 토큰(TOKEN2)이 생성된다(단계(260)). 집적 회로는 디버그 재-인에이블 토큰과 비교 토큰을 비교한다(단계(270)). 디버그 재-인에이블 토큰이 비교 토큰과 일치한다면, 집적 회로에서 디세이블된 디버그 성능이 재-인에이블된다(단계(280)).

[0013] [0017] 본 발명의 보다 상세한 양상들에서, 디버그 재-인에이블 메시지는 제 1 관계자(220)로부터 수신될 수 있고, 개인키는 제 1 관계자에 대한 것일 수도 있다. 대칭키의 제 1 사본은 제 2 관계자(240)에 저장될 수도 있다. 제 1 관계자의 개인키(KPRI)는 제 2 관계자에게 이용 가능하지 않고, 대칭키(KS)는 제 1 관계자에게 이용 가능하지 않다. 고유 식별자는 SoC 디바이스의 일련번호일 수도 있다. 비교 토큰(TOKEN2)은 일련번호 및 대칭키의 제 2 사본을 입력들로서 사용하는 단방향 암호화 함수, 예컨대 SHA256 해시 함수(310)를 기초로 생성될 수도 있다. 대칭키는 SoC 디바이스의 1회 프로그램 가능(OTP) 메모리(254)에 안전하게 저장될 수 있다.

[0014] [0018] 본 발명의 보다 상세한 양상들에서, 제 1 관계자(220)는 SoC 디바이스(210)의 공급자 및/또는 생산자일 수도 있으며, 제 2 관계자(240)는 주문자 상표 부착 생산자(OEM)일 수도 있다.

[0015] [0019] SoC 디바이스(210)의 공급자(생산자)(220)는 메시지들을 서명하기 위한 개인키(KPRI)를 보유하며, 외부 관계자들과 이 개인키를 공유하지 않는다. 공급자가 자신들의 SoC 디바이스들에서 디버그 성능을 언로크/재-인에이블하는 것을 막길 원하는 OEM(240)은 대칭(또는 OEM) 키(KS)를 SoC 디바이스들 내의 OTP 메모리(즉, eFuse, QFPROM 등)에 제공할 수 있다. 대칭키는 각각의 디바이스에 고유할 수도 있고, 또는 디바이스들에 걸쳐 전역적으로 공유될 수도 있다. 이에 따라, 공급기는 SoC 디바이스(210)에서 디버그를 재-인에이블하도록 다음과 같이 진행할 수 있다.

[0016] [0020] 공급자(220)는 칩 일련번호를 명시하는 정식 요청을 OEM(240)에 전달한다(단계(222)). 이는 OTP 메모리(254)에 저장된 고유 일련번호이다. 대안으로, OEM은 우선 공급자에게 고유 일련번호와 함께 반환 제품 승인(RMA: return material authorization)을 전송한다.

[0017] [0021] OEM(240)은 일련번호 및 OEM 키(KS)를 해시함으로써 디바이스별 256 비트 디버그 언로크/재-인에이블 토큰(TOKEN1)을 생성한다(단계(224)). OEM은 이 토큰을 공급기(220)에 제공한다(단계(226)).

[0018] [0022] 공급기(220)는 공급기에만 알려지는 개인키(KPRI)에 의해 서명된 디버그 재-인에이블 메시지를 생성한다. 서명된 메시지는 OEM 제공 토큰(TOKEN1)을 포함한다.

[0019] [0023] SoC 디바이스(210) 내의 키 제공 하드웨어 코어(320)가 메시지에 대해 서명을 인증하고, 디버그 재-인에이블 토큰(TOKEN1)을 풀어 비교기(350)에 출력한다. SoC 하드웨어(HW: hardware)는 또한 OTP 메모리(254)에 저장된 일련번호 및 OEM 키(KS)의 해시를 수행함으로써 256 비트 토큰(TOKEN2)을 생성한다. 수신된 디버그 재-인에이블 토큰(TOKEN1)이 SoC HW 생성된 비교 토큰(TOKEN2)과 일치한다면, 동작(예를 들어, 디버그 재-인에이블)이 허용된다.

[0020] [0024] 본 발명의 기술은 하드웨어에 구현하기에 충분히 간단하고, SoC 디바이스 생산자가 궁극적인 RMA 디버그 제어를 보유하게 하는 동시에, OEM들이 이들이 승인하지 않는 동작들을 차단하게 한다.

[0021] [0025] 도 1과 도 4를 추가로 참조하면, 원격국(102)은 (SoC 디바이스(210)와 같은) 프로세서(410), (메모리 및/또는 디스크 드라이브와 같은) 저장 매체(420), 디스플레이(430), 및 키패드(440)와 같은 입력을 포함하는 컴퓨터(400), 그리고 (Wi-Fi 접속 및/또는 셀룰러 접속과 같은) 무선 접속(450)을 포함할 수도 있다.

[0022] [0026] 본 발명의 다른 양상은 원격국(102)에 있을 수 있는데, 이는: 디버그 재-인에이블 메시지를 수신하기 위한 수단(410) - 메시지는 개인키(KPRI)에 의해 서명된 디버그 재-인에이블 토큰(TOKEN1)을 포함하고, 디버그 재-인에이블 토큰은 집적 회로의 고유 식별자 및 대칭키(KS)의 제 1 사본을 기초로 함 -; 개인키에 대응하는 공개키(KPUB)를 사용하여 디버그 재-인에이블 토큰을 인증하기 위한 수단(410); 고유 식별자를 사용하여 그리고 집적 회로에 안전하게 저장된 대칭키의 제 2 사본을 사용하여 비교 토큰(TOKEN2)을 생성하기 위한 수단(410); 디버그 재-인에이블 토큰과 비교 토큰을 비교하기 위한 수단(410); 및 디버그 재-인에이블 토큰이 비교 토큰과 일치한다면, 집적 회로에서 디세이블된 디버그 성능을 재-인에이블하기 위한 수단(410)을 포함한다.

[0023] [0027] 본 발명의 다른 양상은 원격국(102)에 있을 수 있는데, 이는: 디버그 재-인에이블 메시지를 수신하고 - 메시지는 개인키(KPRI)에 의해 서명된 디버그 재-인에이블 토큰(TOKEN1)을 포함하고, 디버그 재-인에이블 토큰은 단일 칩 시스템(SoC) 디바이스의 고유 식별자 및 대칭키(KS)의 제 1 사본을 기초로 함 -; 개인키에 대응하는 공개키(KPUB)를 사용하여 디버그 재-인에이블 토큰을 인증하고; 고유 식별자를 사용하여 그리고 집적 회로에 안전하게 저장된 대칭키의 제 2 사본을 사용하여 비교 토큰(TOKEN2)을 생성하고; 디버그 재-인에이블 토큰과 비교 토큰을 비교하고; 그리고 디버그 재-인에이블 토큰이 비교 토큰과 일치한다면, 집적 회로에서 디세이블된 디버그 성능을 재-인에이블하도록 구성된 프로세서(410)를 포함한다.

[0024] [0028] 본 발명의 다른 양상은 집적 회로(410)에 있을 수 있는데, 이는: 디버그 재-인에이블 메시지를 수신하기 위한 수단 - 메시지는 개인키(KPRI)에 의해 서명된 디버그 재-인에이블 토큰(TOKEN1)을 포함하고, 디버그 재-인에이블 토큰은 집적 회로의 고유 식별자 및 대칭키(KS)의 제 1 사본을 기초로 함 -; 개인키에 대응하는 공개키(KPUB)를 사용하여 디버그 재-인에이블 토큰을 인증하기 위한 수단; 고유 식별자를 사용하여 그리고 집적 회로에 안전하게 저장된 대칭키의 제 2 사본을 사용하여 비교 토큰(TOKEN2)을 생성하기 위한 수단; 디버그 재-인에이블 토큰과 비교 토큰을 비교하기 위한 수단; 및 디버그 재-인에이블 토큰이 비교 토큰과 일치한다면, 집적 회로에서 디세이블된 디버그 성능을 재-인에이블하기 위한 수단을 포함한다.

[0025] [0029] 디버그 재-인에이블 토큰(TOKEN1)을 전달하는 메시지(MSG)에 대한 서명을 생성하기 위한 방법(500)이 도 5에 도시된다. 메시지 내의 정보가 해시 함수(520), 예를 들어 SHA2 또는 SHA3에 입력되어 다이제스트(530)를 생성한다. 다이제스트는 제 1 관계자(220)의 개인키(KPRI)를 사용하여 메시지 서명 값(550) 생성하기 위한 알고리즘(540)에 입력된다.

[0026] [0030] 도 1을 참조하면, 무선 원격국(RS: remote station)(102)은 무선 통신 시스템(100)의 하나 또는 그보다 많은 기지국(BS: base station)들(104)과 통신할 수 있다. RS는 이동국일 수도 있다. 무선 통신 시스템(100)은 하나 또는 그보다 많은 기지국 제어기(BSC: base station controller)들(106) 및 코어 네트워크(108)를 추가로 포함할 수 있다. 코어 네트워크는 적당한 백홀들을 통해 인터넷(110) 및 공중 전화 교환망(PSTN: Public Switched Telephone Network)(112)에 접속될 수 있다. 일반적인 무선 이동국은 핸드헬드 전화 또는 랩톱 컴퓨터를 포함할 수도 있다. 무선 통신 시스템(100)은 코드 분할 다중 액세스(CDMA: code division multiple access), 시분할 다중 액세스(TDMA: time division multiple access), 주파수 분할 다중 액세스(FDMA: frequency division multiple access), 공간 분할 다중 액세스(SDMA: space division multiple access), 편광 분할 다중 액세스(PDMA: polarization division multiple access) 또는 해당 기술분야에 공지된 다른 변조 기술들과 같은 다수의 다중 액세스 기술 중 임의의 기술을 이용할 수 있다.

[0027] [0031] 해당 기술분야에서 통상의 지식을 가진 자들은, 정보 및 신호들이 다양한 다른 기술들 및 기법들 중 임의의 것을 이용하여 표현될 수 있다고 이해할 것이다. 예를 들어, 상기 설명 전반에 걸쳐 참조될 수 있는 데이터, 명령들, 커맨드들, 정보, 신호들, 비트들, 심벌들 및 칩들은 전압들, 전류들, 전자기파들, 자기 필드들 또는 자기 입자들, 광 필드들 또는 광 입자들, 또는 이들의 임의의 결합들로 표현될 수 있다.

[0028] [0032] 해당 기술분야에서 통상의 지식을 가진 자들은 추가로, 본 명세서에 개시된 실시예들과 관련하여 설명된 다양한 예시적인 로직 블록들, 모듈들, 회로들 및 알고리즘 단계들이 전자 하드웨어, 컴퓨터 소프트웨어, 또는 이 둘의 결합들로 구현될 수 있다고 인식할 것이다. 하드웨어와 소프트웨어의 이러한 상호 호환성을 명확히 설명하기 위해, 각종 예시적인 컴포넌트들, 블록들, 모듈들, 회로들 및 단계들은 일반적으로 이들의 기능과 관련하여 위에서 설명되었다. 이러한 기능이 하드웨어로 구현되는지 아니면 소프트웨어로 구현되는지는 전체 시스템에 부과된 설계 제약들 및 특정 애플리케이션에 좌우된다. 해당 기술분야에서 통상의 지식을 가진 자들은 설명된 기능을 특정 애플리케이션마다 다양한 방식들로 구현할 수도 있지만, 이러한 구현 결정들이 본 발명의 범위를 벗어나게 하는 것으로 해석되지는 않아야 한다.

[0029] [0033] 본 명세서에 개시된 실시예들과 관련하여 설명된 다양한 예시적인 로직 블록들, 모듈들 및 회로들은 범

용 프로세서, 디지털 신호 프로세서(DSP: digital signal processor), 주문형 집적 회로(ASIC: application specific integrated circuit), 필드 프로그래밍 가능 게이트 어레이(FPGA: field programmable gate array) 또는 다른 프로그래밍 가능한 로직 디바이스, 이산 게이트 또는 트랜지스터 로직, 이산 하드웨어 컴포넌트들, 또는 본 명세서에서 설명된 기능들을 수행하도록 설계된 이들의 임의의 결합으로 구현되거나 이들에 의해 수행될 수 있다. 범용 프로세서는 마이크로프로세서일 수도 있지만, 대안으로 프로세서는 임의의 종래 프로세서, 제어기, 마이크로컨트롤러 또는 상태 머신일 수도 있다. 프로세서는 또한 컴퓨팅 디바이스들의 결합, 예를 들어 DSP와 마이크로프로세서의 결합, 복수의 마이크로프로세서들, DSP 코어와 결합된 하나 또는 그보다 많은 마이크로프로세서들, 또는 임의의 다른 이러한 구성으로서 구현될 수도 있다.

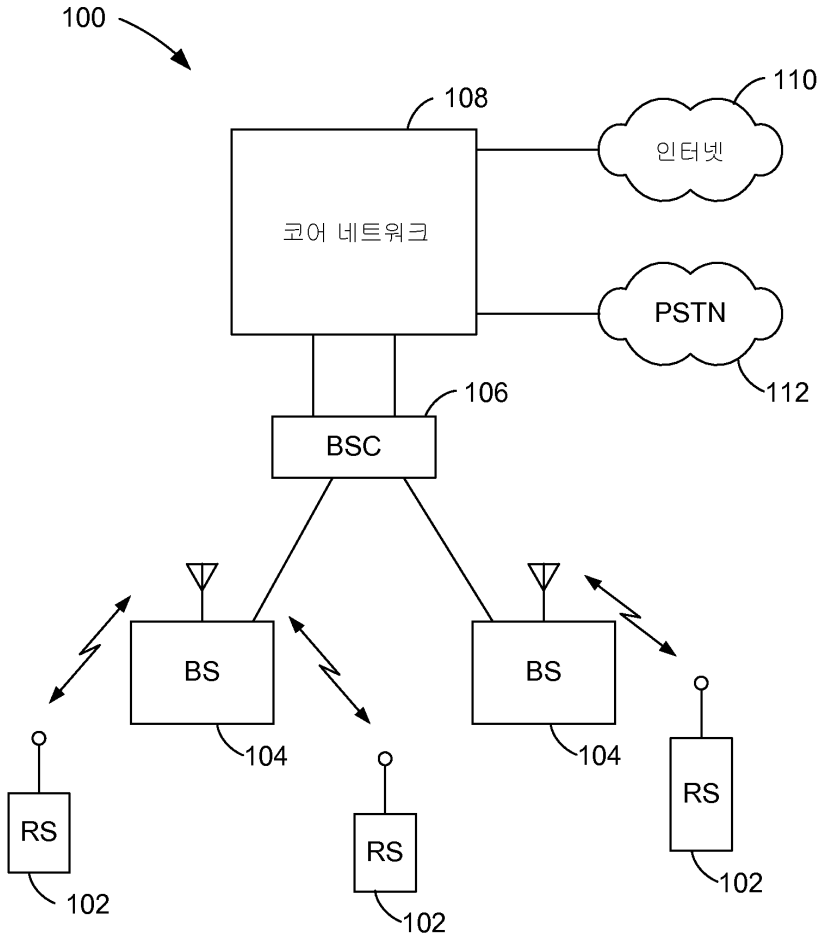
[0030] [0034] 본 명세서에 개시된 실시예들과 관련하여 설명된 방법 또는 알고리즘의 단계들은 직접 하드웨어로, 프로세서에 의해 실행되는 소프트웨어 모듈로, 또는 이 둘의 결합으로 구현될 수 있다. 소프트웨어 모듈은 RAM 메모리, 플래시 메모리, ROM 메모리, EPROM 메모리, EEPROM 메모리, 레지스터들, 하드디스크, 착탈식 디스크, CD-ROM, 또는 해당 기술분야에 공지된 임의의 다른 형태의 저장 매체에 상주할 수 있다. 예시적인 저장 매체는 프로세서가 저장 매체로부터 정보를 읽고 저장 매체에 정보를 기록할 수 있도록 프로세서에 연결된다. 대안으로, 저장 매체는 프로세서에 통합될 수도 있다. 프로세서 및 저장 매체는 ASIC에 상주할 수도 있다. ASIC는 사용자 단말에 상주할 수도 있다. 대안으로, 프로세서 및 저장 매체는 사용자 단말에 개별 컴포넌트들로서 상주할 수도 있다.

[0031] [0035] 하나 또는 그보다 많은 예시적인 실시예들에서, 설명된 기능들은 하드웨어, 소프트웨어, 펌웨어, 또는 이들의 임의의 결합으로 구현될 수도 있다. 컴퓨터 프로그램 물건으로서 소프트웨어로 구현된다면, 이 기능들은 컴퓨터 판독 가능 매체 상에 하나 또는 그보다 많은 명령들 또는 코드로서 저장되거나 이를 통해 송신될 수 있다. 컴퓨터 판독 가능 매체는 한 장소에서 다른 장소로 컴퓨터 프로그램의 전달을 가능하게 하는 임의의 매체를 포함하는 통신 매체와 비-일시적 컴퓨터 저장 매체를 모두 포함한다. 저장 매체는 컴퓨터에 의해 액세스 가능한 임의의 이용 가능한 매체일 수 있다. 제한이 아닌 예로써, 이러한 컴퓨터-판독가능 매체는 RAM, ROM, EEPROM, CD-ROM, 또는 다른 광학 디스크 저장소, 자기 디스크 저장소 또는 다른 자기 저장 디바이스들, 또는 명령들 또는 데이터 구조들의 형태로 요구되는 프로그램 코드를 전달하거나 저장하기 위해 사용될 수 있으며 컴퓨터에 의해 액세스될 수 있는 임의의 다른 매체를 포함할 수 있다. 또한, 임의의 접속이 컴퓨터 판독 가능 매체로 적절히 지칭된다. 예를 들어, 소프트웨어가 동축 케이블, 광섬유 케이블, 꼬임 쌍선, 디지털 가입자 회선(DSL: digital subscriber line), 또는 적외선, 라디오 및 마이크로파와 같은 무선 기술들을 이용하여 웹사이트, 서버 또는 다른 원격 소스로부터 전송된다면, 동축 케이블, 광섬유 케이블, 꼬임 쌍선, DSL, 또는 적외선, 라디오 및 마이크로파와 같은 무선 기술들이 매체의 정의에 포함된다. 본 명세서에서 사용된 것과 같은 디스크(disk 및 disc)는 콤팩트 디스크(CD: compact disc), 레이저 디스크(laser disc), 광 디스크(optical disc), 디지털 다기능 디스크(DVD: digital versatile disc), 플로피 디스크(floppy disk) 및 블루레이 디스크(blu-ray disc)를 포함하며, 여기서 디스크(disk)들은 보통 데이터를 자기적으로 재생하는 한편, 디스크(disc)들은 데이터를 레이저들에 의해 광학적으로 재생한다. 상기의 결합들 또한 컴퓨터 판독 가능 매체의 범위 내에 포함되어야 한다.

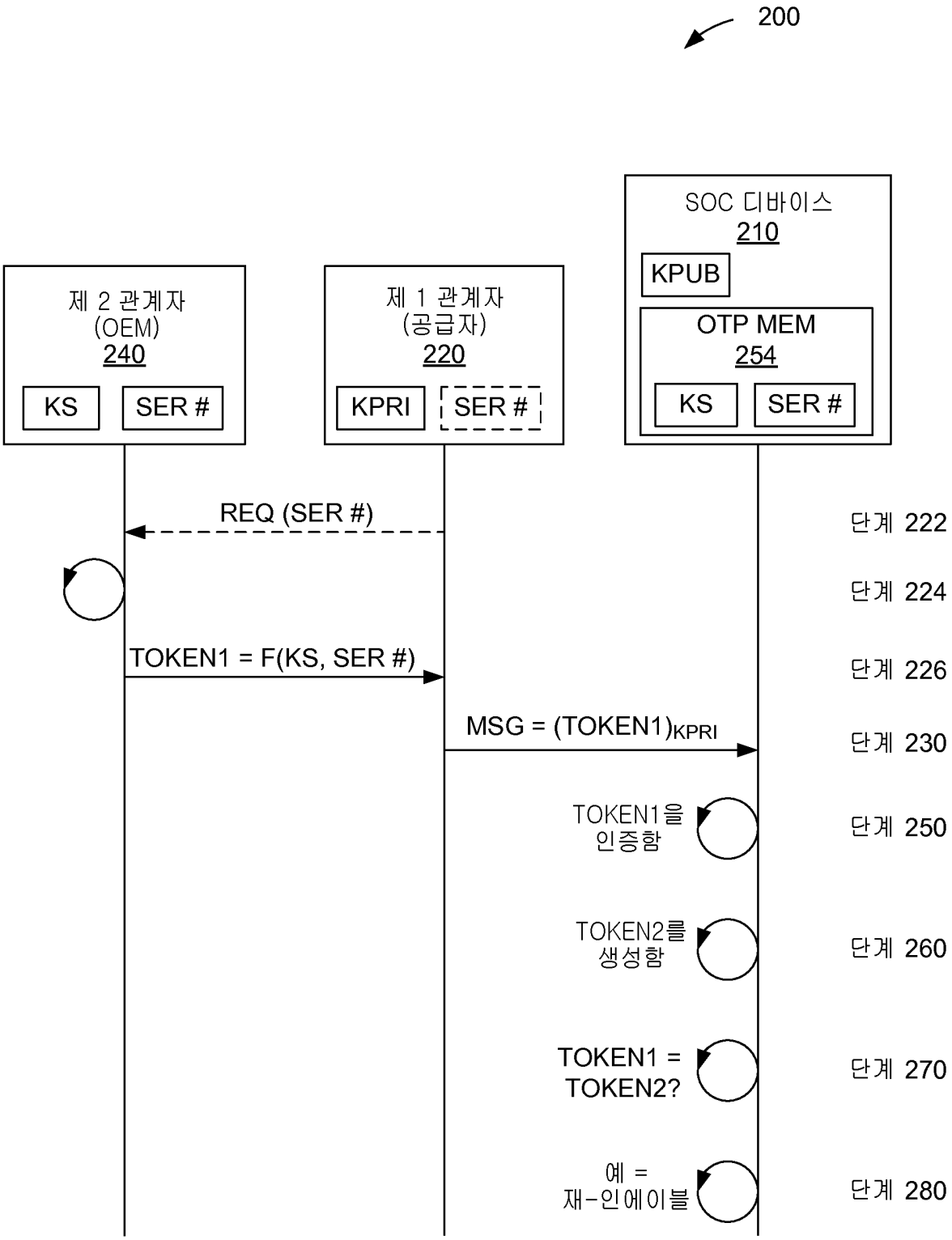
[0032] [0036] 개시된 실시예들의 상기의 설명은 해당 기술분야에서 통상의 지식을 가진 임의의 자가 본 발명을 이용하거나 실시할 수 있게 하도록 제공된다. 이러한 실시예들에 대한 다양한 변형들이 해당 기술분야에서 통상의 지식을 가진 자들에게 쉽게 명백할 것이며, 본 명세서에 정의된 일반 원리들은 본 발명의 진의 또는 범위를 벗어나지 않으면서 다른 실시예들에 적용될 수 있다. 그러므로 본 발명은 본 명세서에 도시된 실시예들로 한정되는 것으로 의도되는 것이 아니라, 본 명세서에 개시된 원리들 및 신규한 특징들에 부합하는 가장 넓은 범위에 따르는 것이다.

도면

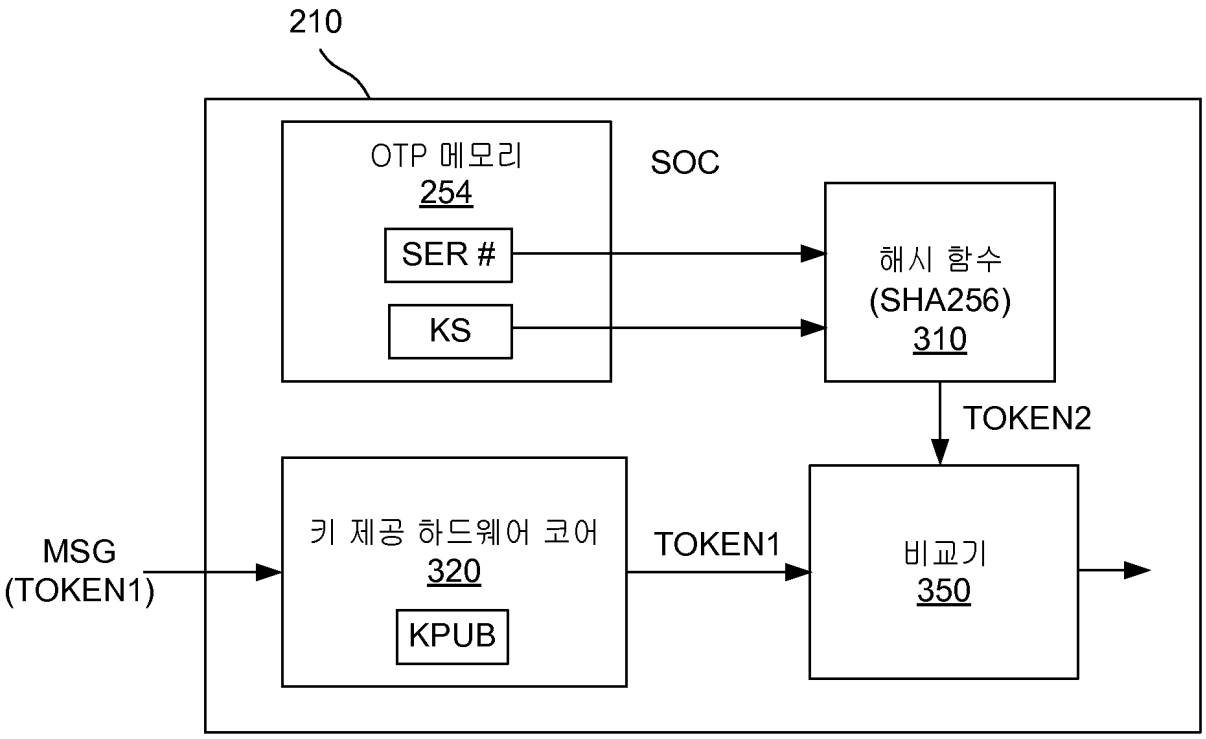
도면1


100
108
110
인터넷
코어 네트워크
PSTN
112
106
BSC
BS
BS
104
104
RS
RS
RS
102
102
102

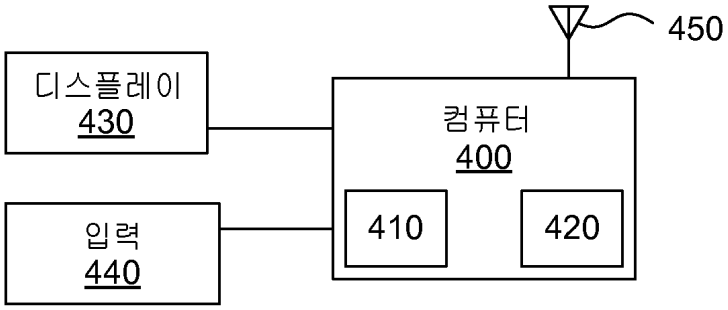
도면2


200
SOC 디바이스
210
KPUB
OTP MEM
254
KS
SER #
제 2 관계자
(OEM)
240
KS
SER #
제 1 관계자
(공급자)
220
KPRI
SER #
REQ (SER #)
단계 222
단계 224
TOKEN1 = F(KS, SER #)
단계 226
MSG = (TOKEN1)KPRI
단계 230
TOKEN1을
인증함
단계 250
TOKEN2를
생성함
단계 260
TOKEN1 =
TOKEN2?
단계 270
예 =
재-인에이블
단계 280

도면3


210
OTP 메모리
254
SER #
KS
SOC
해시 함수
(SHA256)
310
TOKEN2
MSG
(TOKEN1)
키 제공 하드웨어 코어
320
KPUB
TOKEN1
비교기
350

도면4


450
디스플레이
430
입력
440
컴퓨터
400
410
420

도면5