(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0125974
(43) 공개일자 2018년11월26일

(51) 국제특허분류(Int. Cl.)
G06F 17/50 (2006.01) *G06F 21/57* (2013.01)
G06F 21/76 (2013.01)
(52) CPC특허분류
G06F 17/5045 (2013.01)
G06F 21/57 (2013.01)
(21) 출원번호 10-2018-7027690
(22) 출원일자(국제) 2017년03월09일
심사청구일자 없음
(85) 번역문제출일자 2018년09월21일
(86) 국제출원번호 PCT/US2017/021611
(87) 국제공개번호 WO 2017/172322
국제공개일자 2017년10월05일
(30) 우선권주장
62/314,928 2016년03월29일 미국(US)
15/234,879 2016년08월11일 미국(US)

(71) 출원인
퀄컴 인코포레이티드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
맥클린 아이반
미국 92121-1714 캘리포니아주 샌디에고 모어하우스 드라이브 5775
모스코비치 스튜어트
미국 92121-1714 캘리포니아주 샌디에고 모어하우스 드라이브 5775
(뒷면에 계속)
(74) 대리인
특허법인코리아나

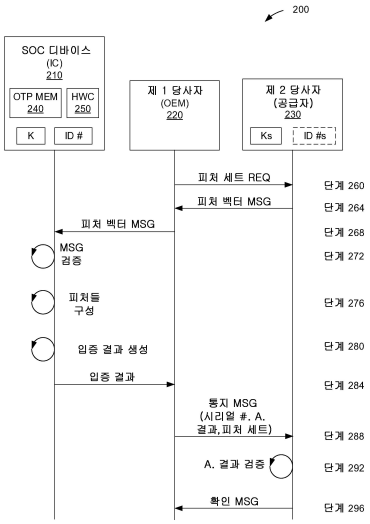
전체 청구항 수 : 총 30 항

(54) 발명의 명칭 **요청된 피처 세트로 집적 회로를 구성하는 방법 및 장치**

(57) 요 약

집적 회로의 피처들을 구성하는 방법이 개시되어 있다. 본 방법에서, 집적 회로는 제 1 당사자로부터 피처 벡터 메시지를 수신한다. 피처 벡터 메시지는 제 1 당사자로부터 제 2 당사자로의 피처 세트 요청에 대한 응답에 포함된다. 집적 회로는 피처 벡터 메시지에서의 피처 벡터에 기초하여 집적 회로의 적어도 하나의 피처를 구성한다. 집적 회로는 집적 회로의 적어도 하나의 구성된 피처에 기초하여 그리고 집적 회로에 보안적으로 저장되고 제 2 당사자에 알려져 있고 제 1 당사자에 알려져 있지 않은 키를 이용하여 입증 결과를 생성한다. 집적 회로는 제 1 당사자에 입증 결과를 포워딩한다.

대 표 도 - 도2



(52) CPC특허분류
G06F 21/76 (2013.01)
(72) 발명자
캠벨 브라이언
미국 92121-1714 캘리포니아주 샌디에고 모어하우스 드라이브 5775

드라기세비치 마크
미국 92121-1714 캘리포니아주 샌디에고 모어하우스 드라이브 5775

명 세 서

청구범위

청구항 1

집적 회로를 구성하는 방법으로서,

상기 집적 회로에 의해, 제 1 당사자로부터 피처 벡터 메시지를 수신하는 단계로서, 상기 피처 벡터 메시지는 상기 제 1 당사자로부터 제 2 당사자로의 피처 세트 요청에 대한 응답에 포함되는, 상기 피처 벡터 메시지를 수신하는 단계;

상기 집적 회로에 의해, 상기 피처 벡터 메시지에서의 피처 벡터에 기초하여 상기 집적 회로의 적어도 하나의 피처를 구성하는 단계;

상기 집적 회로에 의해, 상기 집적 회로의 구성된 상기 적어도 하나의 피처에 기초하여 그리고 상기 집적 회로에 보안적으로 저장되고 상기 제 2 당사자에 알려져 있고 상기 제 1 당사자에 알려져 있지 않은 키를 이용하여 입증 결과를 생성하는 단계; 및

상기 입증 결과를 상기 제 1 당사자에 포워딩하는 단계를 포함하는, 집적 회로를 구성하는 방법.

청구항 2

제 1 항에 있어서,

상기 집적 회로는 SOC (system-on-a-chip) 디바이스인, 집적 회로를 구성하는 방법.

청구항 3

제 1 항에 있어서,

상기 제 1 당사자는 OEM (original equipment manufacturer) 이고, 상기 제 2 당사자는 상기 집적 회로의 공급자인, 집적 회로를 구성하는 방법.

청구항 4

제 1 항에 있어서,

상기 피처 벡터 메시지는 상기 제 2 당사자에 의해 서명되고,

상기 방법은 상기 집적 회로에 의해, 상기 피처 벡터 메시지의 서명을 이용하여 상기 피처 벡터 메시지를 검증하는 단계를 더 포함하는, 집적 회로를 구성하는 방법.

청구항 5

제 1 항에 있어서,

상기 집적 회로는 고유 식별자에 의해 식별되고, 상기 키는 상기 집적 회로에 고유한, 집적 회로를 구성하는 방법.

청구항 6

제 1 항에 있어서,

상기 피처 세트 요청의 피처 세트는 재고 보유 유닛 (stock keeping unit; SKU) 에 대응하는, 집적 회로를 구성하는 방법.

청구항 7

제 1 항에 있어서,

상기 집적 회로에 의해, 적어도 하나의 플래그를 1회 프로그래밍가능 (one-time-programmable; OTP) 메모리에서

설정하는 단계를 더 포함하고, 각각의 설정된 플래그는 상기 집적 회로의 피처와 연관되는, 집적 회로를 구성하는 방법.

청구항 8

제 7 항에 있어서,

상기 OTP 메모리에서 설정된 플래그는 디스에이블된 피처에 대응하는, 집적 회로를 구성하는 방법.

청구항 9

제 7 항에 있어서,

상기 OTP 메모리에서 설정된 플래그는 인에이블된 피처에 대응하는, 집적 회로를 구성하는 방법.

청구항 10

집적 회로로서,

제 1 당사자로부터 피처 벡터 메시지를 수신하기 위한 수단으로서, 상기 피처 벡터 메시지는 상기 제 1 당사자로부터 제 2 당사자로의 피처 세트 요청에 대한 응답에 포함되는, 상기 피처 벡터 메시지를 수신하기 위한 수단;

상기 피처 벡터 메시지에서의 피처 벡터에 기초하여 상기 집적 회로의 적어도 하나의 피처를 구성하기 위한 수단;

상기 집적 회로의 구성된 상기 적어도 하나의 피처에 기초하여 그리고 상기 집적 회로에 보안적으로 저장되고 상기 제 2 당사자에 알려져 있고 상기 제 1 당사자에 알려져 있지 않은 키를 이용하여 입증 결과를 생성하기 위한 수단; 및

상기 입증 결과를 상기 제 1 당사자에 포워딩하기 위한 수단을 포함하는, 집적 회로.

청구항 11

제 10 항에 있어서,

상기 집적 회로는 SOC (system-on-a-chip) 디바이스인, 집적 회로.

청구항 12

제 10 항에 있어서,

상기 제 1 당사자는 OEM (original equipment manufacturer) 이고, 상기 제 2 당사자는 상기 집적 회로의 공급자인, 집적 회로.

청구항 13

제 10 항에 있어서,

상기 피처 벡터 메시지는 상기 제 2 당사자에 의해 서명되고,

상기 집적 회로는 상기 피처 벡터 메시지의 서명을 이용하여 상기 피처 벡터 메시지를 검증하기 위한 수단을 더 포함하는, 집적 회로.

청구항 14

제 10 항에 있어서,

상기 집적 회로는 고유 식별자에 의해 식별되고, 상기 키는 상기 집적 회로에 고유한, 집적 회로.

청구항 15

제 10 항에 있어서,

상기 피처 세트 요청의 피처 세트는 재고 보유 유닛 (SKU) 에 대응하는, 집적 회로.

청구항 16

제 10 항에 있어서,

적어도 하나의 플래그를 1회 프로그래밍가능 (OTP) 메모리에서 설정하기 위한 수단을 더 포함하고, 각각의 설정된 플래그는 상기 집적 회로의 피처와 연관되는, 집적 회로.

청구항 17

제 16 항에 있어서,

상기 OTP 메모리에서 설정된 플래그는 디스에이블된 피처에 대응하는, 집적 회로.

청구항 18

제 16 항에 있어서,

상기 OTP 메모리에서 설정된 플래그는 인에이블된 피처에 대응하는, 집적 회로.

청구항 19

스테이션으로서,

프로세서를 포함하는 집적 회로를 포함하고,

상기 프로세서는:

제 1 당사자로부터 피처 벡터 메시지를 수신하는 것으로서, 상기 피처 벡터 메시지는 상기 제 1 당사자로부터 제 2 당사자로의 피처 세트 요청에 대한 응답에 포함되는, 상기 피처 벡터 메시지를 수신하고;

상기 피처 벡터 메시지에서의 피처 벡터에 기초하여 상기 집적 회로의 적어도 하나의 피처를 구성하고;

상기 집적 회로의 구성된 상기 적어도 하나의 피처에 기초하여 그리고 상기 집적 회로에 보안적으로 저장되고 상기 제 2 당사자에 알려져 있고 상기 제 1 당사자에 알려져 있지 않은 키를 이용하여 입증 결과를 생성하고; 그리고

상기 입증 결과를 상기 제 1 당사자에 포워딩하도록 구성되는, 스테이션.

청구항 20

제 19 항에 있어서,

상기 집적 회로는 SOC (system-on-a-chip) 디바이스인, 스테이션.

청구항 21

제 19 항에 있어서,

상기 제 1 당사자는 OEM (original equipment manufacturer) 과 연관되고, 상기 제 2 당사자는 상기 집적 회로의 공급자와 연관되는, 스테이션.

청구항 22

제 19 항에 있어서,

상기 피처 벡터 메시지는 상기 제 2 당사자에 의해 서명되는, 스테이션.

청구항 23

제 19 항에 있어서,

상기 피처 세트는 재고 보유 유닛 (SKU) 에 대응하는, 스테이션.

청구항 24

제 19 항에 있어서,

상기 키는 하나 보다 많은 집적 회로에 의해 공유되는 글로벌 키인, 스테이션.

청구항 25

스테이션으로서,

프로세서를 포함하고,

상기 프로세서는:

피처 세트에 대한 요청을 다른 스테이션에 포워딩하고;

피처 벡터 메시지를 상기 다른 스테이션으로부터 수신하고;

상기 피처 벡터 메시지를 집적 회로에 포워딩하고;

상기 집적 회로의 적어도 하나의 구성된 피처에 기초하여 그리고 상기 집적 회로에 보안적으로 저장되고 상기 다른 스테이션에 알려져 있고 상기 스테이션에 알려져 있지 않은 키에 추가로 기초하여 입증 결과를 수신하고; 그리고

상기 입증 결과, 상기 피처 세트, 및 상기 집적 회로에 대한 고유 식별자를 상기 다른 스테이션에 포워딩하도록 구성되는, 스테이션.

청구항 26

제 25 항에 있어서,

상기 집적 회로는 SOC (system-on-a-chip) 디바이스인, 스테이션.

청구항 27

제 25 항에 있어서,

상기 스테이션은 OEM (original equipment manufacturer) 과 연관되고, 상기 다른 스테이션은 상기 집적 회로의 공급자와 연관되는, 스테이션.

청구항 28

제 25 항에 있어서,

상기 피처 벡터 메시지는 상기 다른 스테이션에 의해 서명되는, 스테이션.

청구항 29

제 25 항에 있어서,

상기 피처 세트는 재고 보유 유닛 (SKU) 에 대응하는, 스테이션.

청구항 30

제 25 항에 있어서,

상기 키는 하나 보다 많은 집적 회로에 의해 공유되는 글로벌 키인, 스테이션.

발명의 설명

기 술 분 야

[0001] 관련 출원들의 상호 참조

[0002] 본 출원은 2016년 3월 29일 미국 특허청에 제출된 가출원 번호 62/314,928 및 2016년 8월 11일 미국 특허청에

제출된 비가출원 번호 15/234,879 의 이익을 우선권으로 주장하며, 그 전체 내용을 본원에서는 참조로서 포함한다.

[0003] 기술분야

[0004] 본 발명은 일반적으로 OEM (Original Equipment Manufacturer) 에 의해 요청된 피처 세트로 집적 회로를 구성하는 것에 관한 것이다.

배 경 기 술

[0005] 모뎀 시스템-온-칩 (System-on-Chip; SoC) 설계는 수 백 개 또는 심지어 수 천 개 별도의 하드웨어 및 소프트웨어 피처들을 포함할 수도 있다. 이들 피처들은 상이한 마켓들, 표준들, 제품 계층들 (product tiers) 및 사용 케이스들을 어드레싱하도록 구성된다. 일부 피처들은 일부 제품들에 요구되지 않거나 또는 심지어 요망되지 않으며 고객들은 이용되지 않은 피처들에 대해 지불하기를 원하지 않는다. 따라서, 칩 공급자는 많은 상이한 버전들을 생성할 수도 있고 각각의 버전은 피처들의 상이한 서브세트를 지원한다. 그러나, 각각의 버전이 특정 하드웨어 로직을 물리적으로 추가 또는 제거하는 경우, 칩 공급자가 물리적으로 별도의 SoC 버전들을 생성하는 것은 비실용적일 수도 있다.

[0006] 대신에, 각각의 버전이 전체 시장의 넓은 계층을 타겟으로 하도록 의도되는 경우, 공급자는 물리적으로 별도의 SoC 버전들을 만들 수도 있다. 특정한 피처들이 칩 제조 동안 공급자에 의해 인에이블 또는 디스에이블되는 경우, 이들 버전들 각각이 추가로 커스터마이즈될 수도 있다. 그 결과, 물리적으로 동일한 SoC들이 상이한 피처 세트들을 지원할 수도 있고 이에 따라 가격이 매겨질 수도 있다.

[0007] 이는 칩 공급자 및 OEM들 (Original Equipment Manufacturers) 양쪽에 대해 수 개의 상당한 문제들을 일으킨다. 이들은 공급자와 OEM 양쪽에 대한 재고 관리 문제들을 포함한다. 공급자는 주문들을 이행하기에 훨씬 앞서 얼마나 많은 주어진 버전을 제조해야 하는지 정확하게 결정해야 한다. OEM 은 자신들이 얼마나 많은 주어진 모델을 제조해야 하는지를 정확하게 결정해야 한다. 양쪽 당사자들에 의한 이 예측은 어떠한 강제 판매 수치의 이용가능성 보다 몇개월 앞서 수행되어야 한다. OEM 이 너무 적은 부품들을 주문받으면, 이들은 후속 주문들을 이행하는 한편, 제조가 지연될 것이라는 전망을 한다. OEM 이 너무 많이 주문받으면, 이들은 미사용 부품들의 비용을 부담해야 한다. 공급자가 너무 많은 주어진 버전을 제조하면, 이들 칩들은 판매할 수 없는 칩들의 "본 파일" 로 끝날 수도 있다. 또한, 이들 많은 버전들 각각은 제조, 테스트, 물리적 마킹, 저장, 추적 및 수송을 위한 전용 "레인"을 도입할 수도 있다. 하나의 레인에서의 칩들은 다른 레인에서의 칩들과 믹싱되지 않을 수도 있다.

[0008] 따라서, OEM 과 칩 공급자에게 유리한 방식으로 피처들로 집적 회로를 구성하는 기법들이 필요하다.

발명의 내용

해결하려는 과제

과제의 해결 수단

[0009] 본 발명의 일 양태는 집적 회로를 구성하는 방법에서 구현될 수도 있다. 본 방법에서, 집적 회로는 제 1 당사자로부터 피처 벡터 메시지를 수신한다. 피처 벡터 메시지는 제 1 당사자로부터 제 2 당사자로의 피처 세트 요청에 대한 응답에 포함된다. 집적 회로는 피처 벡터 메시지에서의 피처 벡터에 기초하여 집적 회로의 적어도 하나의 피처를 구성한다. 집적 회로는 집적 회로의 적어도 하나의 구성된 피처에 기초하여 그리고 집적 회로에 보안적으로 저장되고 제 2 당사자에 알려져 있고 제 1 당사자에 알려져 있지 않은 키를 이용하여 입증 결과를 생성한다. 집적 회로는 입증 결과를 제 1 당사자에 포워딩할 수도 있다.

[0010] 본 발명의 보다 세부적인 양태들에서, 집적 회로는 시스템-온-칩 (system-on-a-chip; SOC) 디바이스일 수도 있고, 제 1 당사자는 OEM (original equipment manufacturer) 일 수도 있고/있거나 제 2 당사자는 집적 회로의 공급자일 수도 있다. 집적 회로는 고유한 식별자에 의해 식별될 수도 있고, 키는 집적 회로에 고유할 수도 있다. 또한, 피처 세트는 재고 보유 유닛 (stock keeping unit; SKU) 에 대응할 수도 있다.

[0011] 본 발명의 다른 더 세부적인 양태들에서, 피처 벡터 메시지는 제 2 당사자에 의해 서명될 수도 있고, 본 방법은

집적 회로에 의해, 피처 벡터 메시지의 서명을 이용하여 피처 벡터 메시지를 검증하는 단계를 더 포함할 수도 있다. 추가로, 본 방법은 집적 회로에 의해, 적어도 하나의 플래그를 1회 프로그래밍가능 (one-time-programmable; OTP) 메모리에서 설정하는 단계를 더 포함할 수도 있고, 각각의 설정된 플래그는 집적 회로의 피처와 연관된다. OTP 메모리에서의 설정된 플래그는 디스에이블된 피처 또는 인에이블된 피처에 대응할 수도 있다.

[0012] 본 발명의 다른 양태는 집적 회로에서 구현될 수도 있으며, 제 1 당사자로부터 피처 벡터 메시지를 수신하기 위한 수단으로서, 피처 벡터 메시지는 제 1 당사자로부터 제 2 당사자로의 피처 세트 요청에 대한 응답에 포함되는, 상기 피처 벡터 메시지를 수신하기 위한 수단; 피처 벡터 메시지에서의 피처 벡터에 기초하여 집적 회로의 적어도 하나의 피처를 구성하기 위한 수단; 집적 회로의 적어도 하나의 구성된 피처에 기초하여 그리고 집적 회로에 보안적으로 저장되고 제 2 당사자에 알려져 있고 제 1 당사자에 알려져 있지 않은 키를 이용하여 입증 결과를 생성하기 위한 수단; 및 입증 결과를 제 1 당사자에 포워딩하기 위한 수단을 포함한다.

[0013] 본 발명의 다른 양태는 집적 회로에서 구현될 수도 있으며, 제 1 당사자로부터 피처 벡터 메시지를 수신하는 것으로서, 피처 벡터 메시지는 제 1 당사자로부터 제 2 당사자로의 피처 세트 요청에 대한 응답에 포함되는, 상기 피처 벡터 메시지를 수신하고; 피처 벡터 메시지에서의 피처 벡터에 기초하여 집적 회로의 적어도 하나의 피처를 구성하고; 집적 회로의 적어도 하나의 구성된 피처에 기초하여 그리고 집적 회로에 보안적으로 저장되고 제 2 당사자에 알려져 있고 제 1 당사자에 알려져 있지 않은 키를 이용하여 입증 결과를 생성하고; 그리고 입증 결과를 제 1 당사자에 포워딩하도록 구성되는 프로세서를 포함한다.

[0014] 본 발명의 다른 양태는 집적 회로를 구성하는 방법에서 구현될 수도 있다. 본 방법에서, 제 1 당사자는 피처 세트에 대한 요청을 제 2 당사자에 포워딩한다. 응답하여, 제 1 당사자는 제 2 당사자로부터 피처 벡터 메시지를 수신한다. 제 1 당사자는 피처 벡터 메시지를 집적 회로에 포워딩한다. 제 1 당사자는 집적 회로의 적어도 하나의 구성된 피처에 기초하여 그리고 집적 회로에 보안적으로 저장되고 제 2 당사자에 알려져 있고 제 1 당사자에 알려져 있지 않은 키에 추가로 기초하여 입증 결과를 수신한다. 제 1 당사자는 입증 결과, 피처 세트 및 집적 회로에 대한 고유 식별자를 제 2 당사자에 포워딩한다.

[0015] 본 발명의 다른 양태는 스테이션에서 구현될 수도 있고, 피처 세트에 대한 요청을 다른 스테이션에 포워딩하기 위한 수단; 피처 벡터 메시지를 다른 스테이션으로부터 수신하기 위한 수단; 피처 벡터 메시지를 집적 회로에 포워딩하기 위한 수단; 집적 회로의 적어도 하나의 구성된 피처에 기초하여 그리고 집적 회로에 보안적으로 저장되고 다른 스테이션에 알려져 있고 스테이션에 알려져 있지 않은 키에 추가로 기초하여 입증 결과를 수신하기 위한 수단; 및 입증 결과, 피처 세트, 및 집적 회로에 대한 고유 식별자를 다른 스테이션에 포워딩하기 위한 수단을 포함한다.

[0016] 본 발명의 다른 양태는 스테이션에서 구현될 수도 있고, 피처 세트에 대한 요청을 다른 스테이션에 포워딩하고; 피처 벡터 메시지를 다른 스테이션으로부터 수신하고; 피처 벡터 메시지를 집적 회로에 포워딩하고; 집적 회로의 적어도 하나의 구성된 피처에 기초하여 그리고 집적 회로에 보안적으로 저장되고 다른 스테이션에 알려져 있고 스테이션에 알려져 있지 않은 키에 추가로 기초하여 입증 결과를 수신하고; 그리고 입증 결과, 피처 세트, 및 집적 회로에 대한 고유 식별자를 다른 스테이션에 포워딩하도록 구성된 프로세서를 포함한다.

[0017] 본 발명의 다른 양태는 컴퓨터-판독가능 매체에서 구현될 수도 있으며, 컴퓨터로 하여금 피처 세트에 대한 요청을 다른 컴퓨터에 포워딩하게 하는 코드; 컴퓨터로 하여금 피처 벡터 메시지를 다른 컴퓨터로부터 수신하게 하는 코드; 컴퓨터로 하여금 피처 벡터 메시지를 집적 회로에 포워딩하게 하는 코드; 컴퓨터로 하여금 집적 회로의 적어도 하나의 구성된 피처에 기초하여 그리고 집적 회로에 보안적으로 저장되고 다른 컴퓨터에 알려져 있고 컴퓨터에 알려져 있지 않은 키에 추가로 기초하여 입증 결과를 수신하게 하는 코드; 및 컴퓨터로 하여금 입증 결과, 피처 세트, 및 집적 회로에 대한 고유 식별자를 다른 스테이션에 포워딩하게 하는 코드를 포함한다.

[0018] 본 발명의 다른 양태는 집적 회로의 피처들을 검증하는 방법에서 구현될 수도 있다. 본 방법에서, 제 2 당사자는 제 1 당사자로부터 피처 세트에 대한 요청을 수신한다. 제 2 당사자는 피처 벡터 메시지를 제 1 당사자에 포워딩한다. 제 2 당사자는 입증 결과, 피처 세트, 및 집적 회로에 대한 고유 식별자를 제 1 당사자로부터 수신한다. 입증 결과는 집적 회로의 적어도 하나의 구성된 피처에 기초하고, 그리고 집적 회로에 보안적으로 저장되고 제 2 당사자에 알려져 있고 제 1 당사자에 알려져 있지 않은 키에 추가로 기초한다. 제 2 당사자는 키를 이용하여 입증 결과를 검증한다.

[0019] 본 발명의 다른 양태는 스테이션에서 구현될 수도 있고, 다른 스테이션으로부터 피처 세트에 대한 요청을 수신

하기 위한 수단; 피처 벡터 메시지를 다른 스테이션에 포워딩하기 위한 수단; 입증 결과, 피처 세트, 및 집적 회로에 대한 고유 식별자를 다른 스테이션으로부터 수신하기 위한 수단으로서, 입증 결과는 집적 회로의 적어도 하나의 구성된 피처에 기초하고, 그리고 집적 회로에 보안적으로 저장되고 스테이션에 알려져 있고 다른 스테이션에 알려져 있지 않은 키에 추가로 기초하는, 상기 입증 결과, 피처 세트, 및 집적 회로에 대한 고유 식별자를 수신하기 위한 수단; 및 키를 이용하여 입증 결과를 검증하기 위한 수단을 포함한다.

[0020] 본 발명의 다른 양태는 스테이션에서 구현될 수도 있고, 다른 스테이션으로부터 피처 세트에 대한 요청을 수신하고; 피처 벡터 메시지를 다른 스테이션에 포워딩하고; 입증 결과, 피처 세트, 및 집적 회로에 대한 고유 식별자를 다른 스테이션으로부터 수신하는 것으로서, 입증 결과는 집적 회로의 적어도 하나의 구성된 피처에 기초하고, 그리고 집적 회로에 보안적으로 저장되고 스테이션에 알려져 있고 다른 스테이션에 알려져 있지 않은 키에 추가로 기초하는, 상기 입증 결과, 피처 세트, 및 집적 회로에 대한 고유 식별자를 수신하고; 그리고 키를 이용하여 입증 결과를 검증하도록 구성되는 프로세서를 포함한다.

[0021] 본 발명의 다른 양태는 컴퓨터-판독가능 매체에서 구현될 수도 있고, 컴퓨터로 하여금 다른 컴퓨터로부터 피처 세트에 대한 요청을 수신하게 하는 코드; 컴퓨터로 하여금 피처 벡터 메시지를 다른 컴퓨터에 포워딩하게 하는 코드; 컴퓨터로 하여금 입증 결과, 피처 세트, 및 집적 회로에 대한 고유 식별자를 다른 컴퓨터로부터 수신하게 하는 코드로서, 입증 결과는 집적 회로의 적어도 하나의 구성된 피처에 기초하고, 그리고 집적 회로에 보안적으로 저장되고 컴퓨터에 알려져 있고 다른 컴퓨터에 알려져 있지 않은 키에 추가로 기초하는, 상기 입증 결과, 피처 세트, 및 집적 회로에 대한 고유 식별자를 수신하게 하는 코드; 및 컴퓨터로 하여금 키를 이용하여 입증 결과를 검증하게 하는 코드를 포함한다.

도면의 간단한 설명

[0022] 도 1 은 무선 통신 시스템의 일 예의 블록도이다.

도 2 는 본 발명에 따라 요청된 피처 세트로 집적 회로를 구성하는 방법의 흐름도이다.

도 3 은 본 발명에 따라 피처 세트로 집적 회로를 구성하는 방법의 흐름도이다.

도 4 는 피처 벡터 메시지에 대한 서명을 생성하는 방법의 흐름도이다.

도 5 는 입증 결과를 생성하는 방법의 흐름도이다.

도 6 은 프로세서 및 메모리를 포함하는 컴퓨터의 블록도이다.

도 7 은 본 발명에 따라 피처 세트로 집적 회로를 구성하는 다른 방법의 흐름도이다.

도 8 은 본 발명에 따라 집적 회로의 피처들을 검증하는 방법의 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0023] 단어 "예시적인" 은 "예, 예시, 또는 예증의 역할을 하는" 을 의미하는 것으로 본원에서 이용된다. "예시적인" 것으로 본원에서 설명된 임의의 실시형태는 반드시 다른 실시형태들에 비해 바람직하거나 유리한 것으로 해석되는 것은 아니다.

[0024] 도 2 및 도 3 을 참조하여 보면, 본 발명의 일 양태는 집적 회로 (IC)(210) 를 구성하는 방법 (300) 에서 구현될 수도 있다. 본 방법에서, 집적 회로는 제 1 당사자 (220) 로부터 피처 벡터 메시지를 수신한다 (단계 310). 피처 벡터 메시지는 제 1 당사자로부터 제 2 당사자 (230) 로의 피처 세트 요청에 대한 응답에 포함된다. 집적 회로는 피처 벡터 메시지에서의 피처 벡터에 기초하여 집적 회로의 적어도 하나의 피처를 구성한다 (단계 320). 집적 회로는 집적 회로의 적어도 하나의 구성된 피처에 기초하여 그리고 집적 회로에 보안적으로 저장되고 제 2 당사자에 알려져 있고 제 1 당사자에 알려져 있지 않은 키 (K) 를 이용하여 입증 결과를 생성한다 (단계 330). 집적 회로는 입증 결과를 제 1 당사자에 포워딩할 수도 있다 (단계 340).

[0025] 본 발명의 보다 세부적인 양태들에서, 집적 회로 (210) 는 시스템-온-칩 (system-on-a-chip; SOC) 디바이스일 수도 있고, 제 1 당사자 (220) 는 OEM (original equipment manufacturer) 일 수도 있고/있거나 제 2 당사자 (230) 는 집적 회로의 공급자일 수도 있다. 집적 회로는 고유한 식별자 (ID #) 에 의해 식별될 수도 있고, 키는 집적 회로에 고유할 수도 있다. 또한, 피처 세트는 재고 보유 유닛 (stock keeping unit; SKU) 에 대응할 수도 있다.

[0026] 본 발명의 다른 더 세부적인 양태들에서, 피처 벡터 메시지는 제 2 당사자 (230) 에 의해 서명될 수도 있고, 본 방법은 집적 회로 (210) 에 의해, 피처 벡터 메시지의 서명을 이용하여 피처 벡터 메시지를 검증하는 단계를 더 포함할 수도 있다. 추가로, 본 방법은 집적 회로에 의해, 적어도 하나의 플래그를 1회 프로그래밍가능 (one-time-programmable; OTP) 메모리 (240) 에서 설정하는 것을 더 포함할 수도 있고, 각각의 설정된 플래그는 집적 회로의 피처와 연관된다. OTP 메모리에서의 설정된 플래그는 디스에이블된 피처 또는 인에이블된 피처에 대응할 수도 있다.

[0027] 집적 회로 (IC)(210) 는 보안 하드웨어 블록 또는 코어 (secure hardware block or core; HWC)(250) 를 포함할 수도 있다. 적절한 HWC 는 캘리포니아주 샌프란시스코 소재의 CRI (Cryptographic Research, Incorporated) 사에 의해 공급될 수도 있다. HWC 는 비밀 키 (K) 에 대한 배타적 액세스를 홀딩 또는 지닌다. 키는 대칭 키 (예를 들어, AES 키) 일 수도 있거나 또는 프라이빗 키 (예를 들어, RSA 또는 ECC 프라이빗 키) 일 수도 있다. 키는 집적 회로 마다 고유할 수도 있거나 또는 집적 회로에 걸쳐 공유될 수도 있다. OTP (240) 에 저장된 디바이스 당 키는 우수한 보안성을 제공하지만, 공급자/판매자 (230) 에 의한 백엔드 검증은 디바이스 당 키들의 대형 데이터베이스의 관리/룩업을 요구하는 추가된 동작 복잡도를 수반한다. 이와 반대로, 글로벌 공유 키는 키의 노출이 시스템의 보안성을 붕괴하기 때문에 덜 안전하다. 그러나, 글로벌 공유 키는 훨씬더 단순한 백엔드 관리에 기여한다. 키는 집적 회로로부터 추출되지 않을 수 있고 달리, 공급자 (230) 에게만 알려져 있다 (글로벌 키 또는 디바이스/IC 당 키들 (K들)). 구체적으로, 키는 OEM (220) 에 액세스가능하지 않아야 한다. HWC 는 집적 회로의 구성 상태를 영구적으로 저장하는 OTP 메모리 (240) 에 대한 배타적 판독 및 기록 액세스를 갖는다. HWC 는 고유 IC 식별자에 대한 액세스를 가져야 한다. 식별자는 비밀일 필요는 없지만, 그 진위성은 보장되어야 한다. HWC 는 OTP 메모리에 의해 유지된 값들에 대해 서명 또는 HMAC 를 생성가능하다.

[0028] 도 2 에 도시된 방법을 보다 자세하게 참조하여 보면, OEM (220) 은 자신들이 특정 피처 세트 (SKU) 또는 피처 세트들 (SKU들) 의 그룹의 IC들 (210) 을 제조/구성하기 원한다는, IC 공급자/판매자 (즉, 제조자)(230) 에 대한 공식 요청을 행한다 (단계 260). 이 점에서, OEM 은 주어진 피처 세트의 얼마나 많은 IC 가 이들이 제조하려 하는지를 표시할 필요가 없고, 이들은 주어진 피처 세트의 IC 가 실제 구성되는 시간까지 구성 결정을 남겨둘 필요가 없다. OEM 은 공급자로부터 다수의 IC들을 주문받는다. 모든 이들 IC들은 동일한 초기 "디폴트" 구성을 갖는다. 통상적으로, 이들 IC들은 디폴트에 의해 인에이블된 모든 피처들을 갖고, OEM 은 각각의 IC 마다 프라미엄 가격을 지불한다. 그러나, 공급자와 OEM(들) 사이의 비지니스 관계에 따라, 이 접근 방식에 대한 변경이 가능하다. 예를 들어, "디폴트" 구성은 디폴트에 의해 디스에이블된 대부분의 또는 모든 프리미엄 피처들을 가질 수도 있고, 이 경우, OEM 이 "베이스" 구성에 대하여 초기에만 지불한다.

[0029] IC 공급자 (230) 는 IC (210) 의 HWC (250) 에 의해 해석될 피처 벡터 메시지를 생성한다. 메시지는 OEM 에 의해 요청된 피처 세트에 대응하는 고유 피처 벡터를 포함한다. 도 4 를 참조하여 보면, 메시지는 디지털 방식으로 서명될 수도 있다 (그러나 그럴 필요가 없다). 서명은 키 함수 (440), 이를 테면, RSA 알고리즘을 이용하여 메시지 상에서 생성될 수도 있다. 프라이빗 키는 대응하는 공개 키를 가질 수도 있고, 입증 결과를 생성하는데 이용된 키 (K) 에 관련되지 않을 수도 있다. 메시지 서명은 HWC 가 이를 프로세싱하기 전에 HWC 에 의해 검증될 수도 있다. 메시지는 암호화될 필요는 없지만, 그 진위성이 보장되어야 한다. 공급자는 피처 벡터 메시지를 OEM 에 포워딩한다 (단계 264).

[0030] 디바이스 제조 프로세스와 동시에, OEM (220) 은 IC (210) 의 HWC (250) 로 메시지를 피드한다 (단계 268). 동일한 글로벌 메시지가 고유 피처 세트 (SKU) 하에서 구성된 각각의 IC 로 피드될 수도 있다. 메시지를 로딩하기 위한 메카니즘은 OEM 이 담당한다. 예를 들어, 메시지는 IC 상의 파일에 저장되거나 또는 SW 이미지 내에 내장되거나 또는 외부 테스터로부터 IC 로 피드될 수 있다.

[0031] HWC (250) 는 피처 벡터 메시지를 검증할 수 있다 (이는 서명을 체크할 수도 있다)(단계 272). 그후, HWC 는 미리 정의된 비휘발성 "라이프 사이클 비트" 가 설정되지 않음을 체크한다. 이것이 설정되면, HWC 는 동작을 만료한다. 이것이 설정되지 않으면, HWC 는 피처 벡터를 메시지 페이로드로부터 취출하고 이 피처 벡터를 OTP 메모리 (240) 에 (예를 들어, 적절한 퓨즈 비트들 미만으로) 기록한다 (단계 276). 피처 플래그들 (feature flags; FF) 또는 비트들은 도 5 에 도시되어 있다. 플래그들은 모뎀 능력들 (예를 들어, CDMA 또는 UMTS) 을 활성화 또는 비활성화하는 것, (예를 들어, 캐리어 애그리게이션을 통하여) 최대 모뎀 데이터 대역폭을 설정하는 것, 프로세서 (CPU) 를 턴온 또는 턴오프하는 것, 최대 디스플레이 해상도를 설정하는 것, 최대 카메라 해상도를 설정하는 것, 또는 소프트웨어 피처들을 활성화 또는 비활성화하는 것과 같이 특정

피처들에 대응할 수도 있다. 그 후, HWC 는 미리 정의된 라이프사이클 비트를 설정한다.

[0032] 라이프사이클 비트의 역할은 임의의/모든 피처 벡터 메시지들이 HWC (250) 에 의해 한번만 소비될 수 있음을 보장하는 것이다. 이는 동일한 IC (210) 로 다수의 피처 벡터 메시지들을 이용하여 그리고 최저 피처링된 결과만을 보고하는 것에 의해 OEM (220) 에 의한 특정 공격들을 방지한다. 그 후, HWC 는 OTP 로부터 고유 칩 ID 를 판독하고, 칩 ID 및 피처 벡터 값들을 통하여 서명 또는 HMAC들을 행한다 (단계 280). 또한 도 5 를 참조하여 본다. HMAC 는 AES-256 알고리즘을 이용할 수도 있고, 서명은 RSA 알고리즘을 이용할 수도 있다. 결과적인 서명/키잉된 다이제스트 (입증 결과) 가 HWC 에 의해 엑스포트된다. OEM 은 이 HWC 입증된 결과를 판독 및 레코딩한다 (단계 284).

[0033] 각각의 IC (210) 에 대하여, OEM (220) 은 공급자 (230) 에게 <칩 ID, 입증된 결과, 요청된 피처 세트> 트리플릿을 제공한다 (단계 288). 칩 공급자는 그후, 예상된 결과를 특정된 칩 ID 및 피처 세트에 대한 OEM 공급된 결과에 대하여 검증한다 (단계 292). 값들이 매칭하면, 공급자는 확인 메시지를 OEM 에 포워딩한다 (단계 296).

[0034] 예들로서, 공급자 (230) 는 미사용된 피처들의 모두에 대한 리베이트 (rebate) 를 OEM (220) 에 발행할 수도 있다. 그러나, 값이 예상된 결과에 매칭하지 못하면, 이는 불법적 구성 시도를 표시할 수 있고, 공급자는 적절한 액션을 취할 수도 있다.

[0035] 도 2 에 도시된 기법은 제조 동안 OEM (220) 에 의한 "무재고 생산 방식 (just-in-time)" IC 구성을 허용한다. IC/SoC (210) 의 HWC (250) 는 정적 피처 벡터 메시지를 수신하고 입증 결과를 리턴한다. 이 능력은 공급자에게 "라이브" 접속에 대한 필요 없이 그리고 안전한 인프라스트럭처를 배치 및 동작할 필요 없이 지원된다. 즉, 종점들에서만, HWC (250) 및 공급자 (230) 가 보안될 필요가 있다. OEM (220) 과의 통신 접속은 보안적 또는 라이브일 필요는 없다. 추가로, 이 기법은 OEM 에 대한 복잡성 및 테스트 시간 오버헤드를 최소화한다. 각각의 IC/SoC (210) 는 단일 라운드 트립 프로토콜을 이용하여 구성되고, 프로토콜은 어떠한 오프-칩 또는 온-칩 엔티티에 의해 실행될 수도 있다. 프로토콜은 OEM의 기존 플로우들과 가장 잘 맞추어진 시간에, 제조 프로세스 동안 언제든지 트리거링될 수도 있다.

[0036] 본 발명의 다른 양태는 집적 회로 (210) 에서 구현될 수도 있으며, 제 1 당사자 (220) 로부터 피처 벡터 메시지를 수신하기 위한 수단 (예를 들어, HWC (250)) 으로서, 피처 벡터 메시지는 제 1 당사자로부터 제 2 당사자 (230) 로의 피처 세트 요청에 대한 응답에 포함되는, 상기 피처 벡터 메시지를 수신하기 위한 수단; 피처 벡터 메시지에서의 피처 벡터에 기초하여 집적 회로의 적어도 하나의 피처를 구성하기 위한 수단 (예를 들어, HWC (250)); 집적 회로의 적어도 하나의 구성된 피처에 기초하여 그리고 집적 회로에 보안적으로 저장되고 제 2 당사자에 알려져 있고 제 1 당사자에 알려져 있지 않은 키를 이용하여 입증 결과를 생성하기 위한 수단 (예를 들어, HWC (250)); 및 입증 결과를 제 1 당사자에 포워딩하기 위한 수단 (예를 들어, HWC (250)) 을 포함한다.

[0037] 본 발명의 다른 양태는 집적 회로에서 구현될 수도 있으며, 제 1 당사자로부터 피처 벡터 메시지를 수신하는 것으로서, 피처 벡터 메시지는 제 1 당사자로부터 제 2 당사자로의 피처 세트 요청에 대한 응답에 포함되는, 상기 피처 벡터 메시지를 수신하고; 피처 벡터 메시지에서의 피처 벡터에 기초하여 집적 회로의 적어도 하나의 피처를 구성하고; 집적 회로의 적어도 하나의 구성된 피처에 기초하여 그리고 집적 회로에 보안적으로 저장되고 제 2 당사자에 알려져 있고 제 1 당사자에 알려져 있지 않은 키를 이용하여 입증 결과를 생성하고; 그리고 입증 결과를 제 1 당사자에 포워딩하도록 구성되는 프로세서 (예를 들어, HWC (250)) 를 포함한다.

[0038] 원격 스테이션 (102; 도 1) 은 프로세서 (610), 저장 매체 (620), 이를 테면, 메모리 및/또는 디스크 드라이브, 디스플레이 (630), 및 입력, 이를 테면, 키패드 (640) 및 무선 접속 (650) 을 포함하는 컴퓨터 (600) 를 포함할 수도 있다.

[0039] 도 2 및 도 7 을 참조하여 보면, 본 발명의 다른 양태는 집적 회로 (210) 를 구성하는 방법 (700) 에서 구현될 수도 있다. 본 방법에서, 제 1 당사자 (220) 는 피처 세트에 대한 요청을 제 2 당사자 (230) 에 포워딩한다 (단계 710). 응답하여, 제 1 당사자는 제 2 당사자로부터 피처 벡터 메시지를 수신한다 (단계 720). 제 1 당사자는 피처 벡터 메시지를 집적 회로에 포워딩한다 (단계 730). 제 1 당사자는 집적 회로의 적어도 하나의 구성된 피처에 기초하여 그리고 집적 회로에 보안적으로 저장되고 제 2 당사자에 알려져 있고 제 1 당사자에 알려져 있지 않은 키에 추가로 기초하여 입증 결과를 수신한다 (단계 740). 제 1 당사자는 입증 결과, 피처 세트 및 집적 회로에 대한 고유 식별자를 제 2 당사자에 포워딩한다 (단계 750).

[0040] 본 발명의 다른 양태는 제 1 당사자 (220) 의 스테이션 (예를 들어, 컴퓨터 (600)) 에서 구현될 수도 있고, 피

처 세트에 대한 요청을 제 2 당사자 (230) 의 다른 스테이션에 포워딩하기 위한 수단 (예를 들어, 프로세서 (610)); 피처 벡터 메시지를 다른 스테이션으로부터 수신하기 위한 수단 (예를 들어, 프로세서 (610)); 피처 벡터 메시지를 집적 회로 (210) 에 포워딩하기 위한 수단 (예를 들어, 프로세서 (610)); 집적 회로의 적어도 하나의 구성된 피처에 기초하여 그리고 집적 회로에 보안적으로 저장되고 다른 스테이션에 알려져 있고 스테이션에 알려져 있지 않은 키에 추가로 기초하여 입증 결과를 수신하기 위한 수단 (예를 들어, 프로세서 (610)); 및 입증 결과, 피처 세트, 및 집적 회로에 대한 고유 식별자를 다른 스테이션에 포워딩하기 위한 수단 (예를 들어, 프로세서 (610)) 을 포함한다.

[0041] 본 발명의 다른 양태는 제 1 당사자 (220) 의 스테이션 (예를 들어, 컴퓨터 (600)) 에서 구현될 수도 있고, 피처 세트에 대한 요청을 제 2 당사자 (230) 의 다른 스테이션에 포워딩하고; 피처 벡터 메시지를 다른 스테이션으로부터 수신하고; 피처 벡터 메시지를 집적 회로 (210) 에 포워딩하고; 집적 회로의 적어도 하나의 구성된 피처에 기초하여 그리고 집적 회로에 보안적으로 저장되고 다른 스테이션에 알려져 있고 스테이션에 알려져 있지 않은 키에 추가로 기초하여 입증 결과를 수신하고; 그리고 입증 결과, 피처 세트, 및 집적 회로에 대한 고유 식별자를 다른 스테이션에 포워딩하도록 구성된 프로세서 (예를 들어, 프로세서 (610)) 를 포함한다.

[0042] 본 발명의 다른 양태는 컴퓨터-판독가능 매체 (예를 들어, 저장 매체 (620)) 에서 구현될 수도 있으며, 제 1 당사자 (220) 의 컴퓨터 (예를 들어, 600) 로 하여금 피처 세트에 대한 요청을 제 2 당사자 (230) 의 다른 컴퓨터에 포워딩하게 하는 코드; 컴퓨터로 하여금 피처 벡터 메시지를 다른 컴퓨터로부터 수신하게 하는 코드; 컴퓨터로 하여금 피처 벡터 메시지를 집적 회로에 포워딩하게 하는 코드; 컴퓨터로 하여금 집적 회로 (210) 의 적어도 하나의 구성된 피처에 기초하여 그리고 집적 회로에 보안적으로 저장되고 다른 컴퓨터에 알려져 있고 컴퓨터에 알려져 있지 않은 키에 추가로 기초하여 입증 결과를 수신하게 하는 코드; 및 컴퓨터로 하여금 입증 결과, 피처 세트, 및 집적 회로에 대한 고유 식별자를 다른 스테이션에 포워딩하게 하는 코드를 포함한다.

[0043] 도 2 및 도 8 을 참조하여 보면, 본 발명의 다른 양태는 집적 회로 (210) 의 피처들을 검증하는 방법 (800) 에서 구현될 수도 있다. 본 방법에서, 제 2 당사자는 제 1 당사자로부터 피처 세트에 대한 요청을 수신한다 (단계 810). 제 2 당사자는 피처 벡터 메시지를 제 1 당사자에 포워딩한다 (단계 820). 제 2 당사자는 입증 결과, 피처 세트, 및 집적 회로에 대한 고유 식별자를 제 1 당사자로부터 수신한다 (단계 830). 입증 결과는 집적 회로의 적어도 하나의 구성된 피처에 기초하고, 그리고 집적 회로에 보안적으로 저장되고 제 2 당사자에 알려져 있고 제 1 당사자에 알려져 있지 않은 키에 추가로 기초한다. 제 2 당사자는 키를 이용하여 입증 결과를 검증한다 (단계 840).

[0044] 본 발명의 다른 양태는 제 2 당사자 (230) 의 스테이션 (예를 들어, 컴퓨터 (600) 과 같은 다른 컴퓨터) 에서 구현될 수도 있고, 제 1 당사자 (220) 의 다른 스테이션으로부터 피처 세트에 대한 요청을 수신하기 위한 수단 (예를 들어, 프로세서 (610)); 피처 벡터 메시지를 다른 스테이션에 포워딩하기 위한 수단 (예를 들어, 프로세서 (610)); 입증 결과, 피처 세트, 및 집적 회로 (210) 에 대한 고유 식별자를 다른 스테이션으로부터 수신하기 위한 수단 (예를 들어, 프로세서 (610)) 으로서, 입증 결과는 집적 회로의 적어도 하나의 구성된 피처에 기초하고, 그리고 집적 회로에 보안적으로 저장되고 스테이션에 알려져 있고 다른 스테이션에 알려져 있지 않은 키에 추가로 기초하는, 상기 입증 결과, 피처 세트, 및 집적 회로에 대한 고유 식별자를 수신하기 위한 수단; 및 키를 이용하여 입증 결과를 검증하기 위한 수단 (예를 들어, 프로세서 (610)) 을 포함한다.

[0045] 본 발명의 다른 양태는 제 2 당사자 (230) 의 스테이션 (예를 들어, 컴퓨터 (600) 과 같은 다른 컴퓨터) 에서 구현될 수도 있고, 제 1 당사자 (220) 의 다른 스테이션으로부터 피처 세트에 대한 요청을 수신하고; 피처 벡터 메시지를 다른 스테이션에 포워딩하고; 입증 결과, 피처 세트, 및 집적 회로 (210) 에 대한 고유 식별자를 다른 스테이션으로부터 수신하는 것으로서, 입증 결과는 집적 회로의 적어도 하나의 구성된 피처에 기초하고, 그리고 집적 회로에 보안적으로 저장되고 스테이션에 알려져 있고 다른 스테이션에 알려져 있지 않은 키에 추가로 기초하는, 상기 입증 결과, 피처 세트, 및 집적 회로에 대한 고유 식별자를 수신하고; 그리고 키를 이용하여 입증 결과를 검증하도록 구성된 프로세서 (예를 들어, 프로세서 (610)) 를 포함한다.

[0046] 본 발명의 다른 양태는 컴퓨터-판독가능 매체 (예를 들어, 저장 매체) 에서 구현될 수도 있고, 제 2 당사자 (230) 의 컴퓨터 (예를 들어, 600) 로 하여금 제 1 당사자 (220) 의 다른 컴퓨터로부터 피처 세트에 대한 요청을 수신하게 하는 코드; 컴퓨터로 하여금 피처 벡터 메시지를 다른 컴퓨터에 포워딩하게 하는 코드; 컴퓨터로 하여금 입증 결과, 피처 세트, 및 집적 회로 (210) 에 대한 고유 식별자를 다른 컴퓨터로부터 수신하게 하는 코드로서, 입증 결과는 집적 회로의 적어도 하나의 구성된 피처에 기초하고, 그리고 집적 회로에 보안적으로 저장되고 컴퓨터에 알려져 있고 다른 컴퓨터에 알려져 있지 않은 키에 추가로 기초하는, 상기 입증 결과, 피처

세트, 및 집적 회로에 대한 고유 식별자를 수신하게 하는 코드; 및 컴퓨터로 하여금 키를 이용하여 입증 결과를 검증하게 하는 코드를 포함한다.

[0047] 도 1 을 참조하면, 무선 원격 스테이션 (remote station; RS)(102) 은 무선 통신 시스템 (100) 의 하나 이상의 기지국들 (base station; BS)(104) 과 통신할 수도 있다. 이동국은 SoC (210) 를 포함할 수도 있다. 무선 통신 시스템 (100) 은 하나 이상의 기지국 제어기들 (base station controller; BSC)(106), 및 코어 네트워크 (108) 를 더 포함할 수도 있다. 코어 네트워크는 적절한 백홀들을 통해 인터넷 (110) 및 공중 교환 전화망 (Public Switched Telephone Network; PSTN)(112) 에 접속될 수도 있다. 통상적인 무선 이동국은 핸드헬드 폰, 또는 랩톱 컴퓨터를 포함할 수도 있다. 무선 통신 시스템 (100) 은 코드 분할 다중 접속 (code division multiple access; CDMA), 시간 분할 다중 접속 (time division multiple access; TDMA), 주파수 분할 다중 접속 (frequency division multiple access; FDMA), 공간 분할 다중 접속 (space division multiple access; SDMA), 편파 분할 다중 접속 (polarization division multiple access; PDMA) 과 같은 다수의 액세스 기법들, 또는 공지된 다른 변조 기법들 중 임의의 하나를 사용할 수도 있다.

[0048] 당업자라면, 정보 및 신호들이 임의의 다양한 다른 기술들 및 기법들을 사용하여 표현될 수도 있음을 이해할 것이다. 예를 들면, 상기 설명을 통해 참조될 수도 있는 데이터, 명령들, 커맨드들, 정보, 신호들, 비트들, 심볼들, 및 칩들은 전압들, 전류들, 전자기파들, 자기장들 또는 자기 입자들, 광학 필드들 또는 입자들, 이들의 임의의 조합에 의해 표현될 수도 있다.

[0049] 본원에서 개시된 실시형태들과 연계하여 설명된 다양한 예증적인 논리 블록들, 모듈들, 회로들, 및 알고리즘 단계들이 전자 하드웨어, 컴퓨터 소프트웨어, 또는 양자 모두의 조합들로서 구현될 수도 있다는 것을 당업자들은 또한 알 수 있을 것이다. 하드웨어 및 소프트웨어의 이러한 상호 교환성을 명확하게 설명하기 위해, 다양한 예시적인 컴포넌트들, 블록들, 모듈들, 회로들, 및 단계들을 그들의 기능적 관점에서 일반적으로 위에서 설명되었다. 그러한 기능이 하드웨어 또는 소프트웨어로 구현되는지 여부는 특정 애플리케이션 및 전체 시스템에 부과되는 설계 제약들에 따라 달라진다. 당업자라면, 상술한 기능성을 각각의 특정 어플리케이션에 대해 다양한 방식으로 구현할 수도 있지만, 이러한 구현 결정은 본 발명의 범위를 벗어나게 하는 것으로 이해되어서는 안된다.

[0050] 본원에서 개시된 실시형태들과 연계하여 설명된 다양한 예증적인 논리 블록들, 모듈들, 및 회로들은 범용 프로세서, 디지털 신호 프로세서 (digital signal processor; DSP), 주문형 반도체 (application specific integrated circuit; ASIC), 필드 프로그래머블 게이트 어레이 (field programmable gate array; FPGA) 혹은 다른 프로그래머블 로직 디바이스, 이산 게이트 혹은 트랜지스터 로직, 이산 하드웨어 컴포넌트들, 또는 본원에서 개시된 기능들을 수행하도록 디자인된 것들의 임의의 조합에 의해 구현되거나 수행될 수도 있다. 범용 프로세서는 마이크로프로세서일 수도 있지만, 대안으로서, 프로세서는 임의의 통상의 프로세서, 제어기, 마이크로컨트롤러, 또는 상태 머신일 수도 있다. 프로세서는 또한 컴퓨팅 디바이스들의 조합, 예를 들면, DSP와 마이크로프로세서의 조합, 복수의 마이크로프로세서들, DSP 코어와 연계한 하나 이상의 마이크로프로세서들, 또는 임의의 다른 그러한 구성으로 구현될 수도 있다.

[0051] 본원에서 개시된 실시형태들과 연계하여 설명된 일 방법 또는 알고리즘의 단계들은 하드웨어에서, 프로세서에 의해 실행되는 소프트웨어 모듈에서, 또는 이들 양자의 조합에서 직접적으로 구현될 수도 있다. 소프트웨어 모듈은 RAM 메모리, 플래시 메모리, ROM 메모리, EPROM 메모리, EEPROM 메모리, 레지스터들, 하드 디스크, 이동식 디스크, CD-ROM, 또는 공지된 임의의 다른 형태의 저장 매체 내에 상주할 수도 있다. 예시적인 저장 매체는, 프로세서가 저장 매체로부터 정보를 판독하고, 저장 매체에 정보를 기록할 수 있도록 프로세서에 커플링된다. 대안에서, 저장 매체는 프로세서에 통합될 수도 있다. 프로세서와 저장 매체는 ASIC 내에 있을 수도 있다. ASIC 은 사용자 단말기 내에 있을 수도 있다. 대안에서, 프로세서와 저장 매체는 사용자 단말기에서 개별 컴포넌트들로 있을 수도 있다.

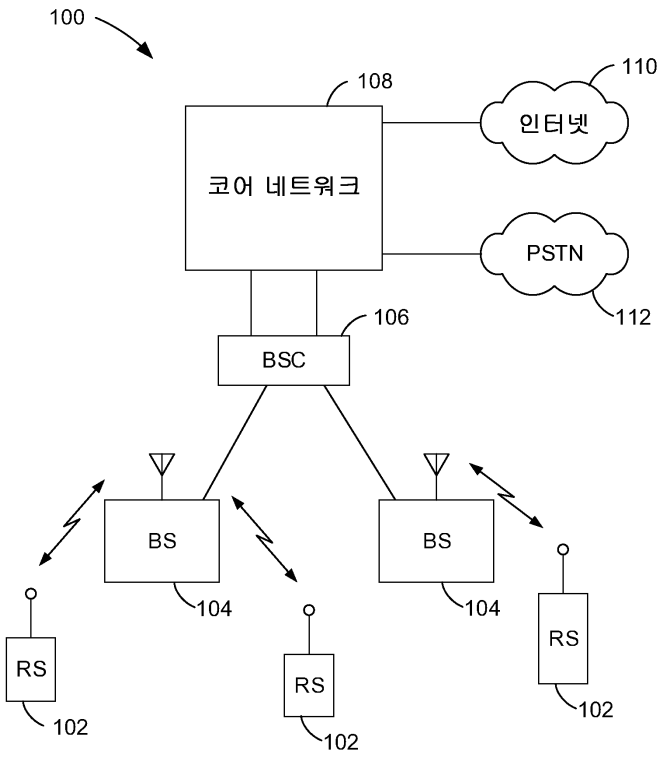
[0052] 하나 이상의 예시적인 실시형태들에서, 상술된 기능들은 하드웨어, 소프트웨어, 펌웨어 또는 이들의 임의의 조합으로 구현될 수도 있다. 컴퓨터 프로그램 제품으로서 소프트웨어로 구현되는 경우, 상기 기능들은 하나 이상의 명령들 또는 코드로서 컴퓨터 판독 가능한 매체 상에 저장되거나 또는 전송될 수도 있다. 컴퓨터 판독가능 매체들은 한 장소에서 다른 장소로 컴퓨터 프로그램의 전송을 가능하게 하는 임의의 매체를 포함한, 통신 매체들 및 비일시적 컴퓨터 저장 매체들 양쪽 모두를 포함한다. 저장 매체는 컴퓨터에 의해 액세스될 수 있는 임의의 이용 가능한 매체일 수도 있다. 비제한적인 예로서, 이러한 컴퓨터 판독 가능한 매체는 RAM, ROM, EEPROM, CD-ROM 또는 다른 광학 디스크 스토리지, 자기 디스크 저장부 또는 다른 자기 저장 디바이스

들, 또는 요구되는 프로그램 코드를 명령들 또는 데이터 구조들의 형태로 이송 또는 저장하기 위해 사용될 수 있으며 컴퓨터에 의해 액세스될 수 있는 임의의 다른 매체를 포함할 수 있다. 또한, 임의의 접속은 컴퓨터 판독 가능한 매체라고 적절히 지칭된다. 예를 들면, 소프트웨어가 동축 케이블, 광섬유 케이블, 연선, 디지털 가입자 회선, 또는 적외선, 무선, 및 마이크로파와 같은 무선 기술들을 사용하여 웹사이트, 서버, 또는 다른 원격 소스로부터 전송되면, 동축 케이블, 광섬유 케이블, 연선, 디지털 가입자 회선, 또는 적외선, 무선, 및 마이크로파와 같은 무선 기술들은 매체의 정의 내에 포함된다. 본원에서 사용된 디스크 (disk) 와 디스크 (disc) 는, 컴팩트 디스크 (CD), 레이저 디스크, 광학 디스크, 디지털 다기능 디스크 (DVD), 플로피디스크 및 블루레이 디스크를 포함하며, 여기서 디스크 (disk) 들은 통상 자기적으로 데이터를 재생하는 반면, 디스크 (disc) 들은 레이저들을 이용하여 광학적으로 데이터를 재생한다. 위의 조합들도 컴퓨터 판독가능 매체들의 범위 내에 포함되어야 한다.

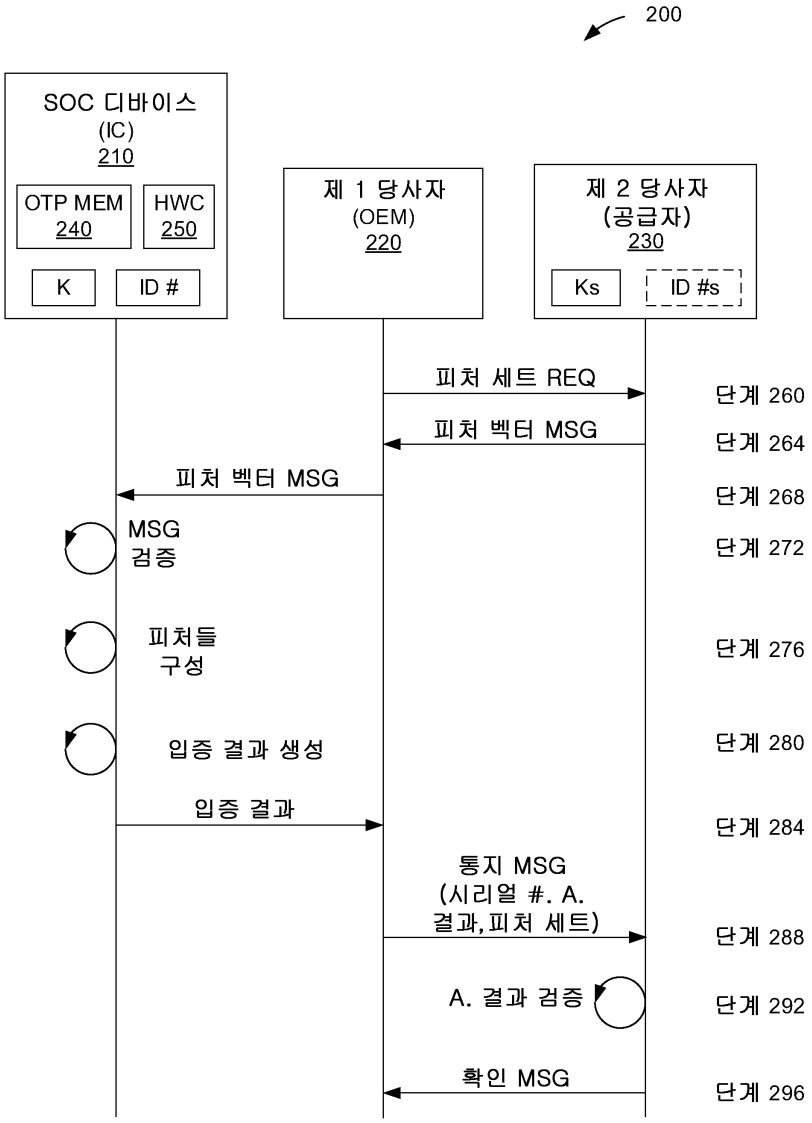
[0053] 개시된 실시형태들의 앞서의 설명들은 임의의 당업자가 본 발명을 실시하거나 이용하는 것을 가능하게 하도록 하기 위해 제공된다. 이러한 실시형태들에 대한 다양한 수정예들이 당업자에게는 자명할 것이고, 본원에서 정의된 일반적인 원칙들은 본 발명의 취지와 범위를 벗어나지 않으면서 다른 실시형태들에 적용될 수도 있다. 따라서, 본 발명은 본원에서 보여진 예시적인 실시형태들로 제한되도록 의도된 것은 아니며 본원의 개시된 원칙들과 신규의 특징들에 부합하는 광의의 범위를 제공하기 위한 것이다.

도면

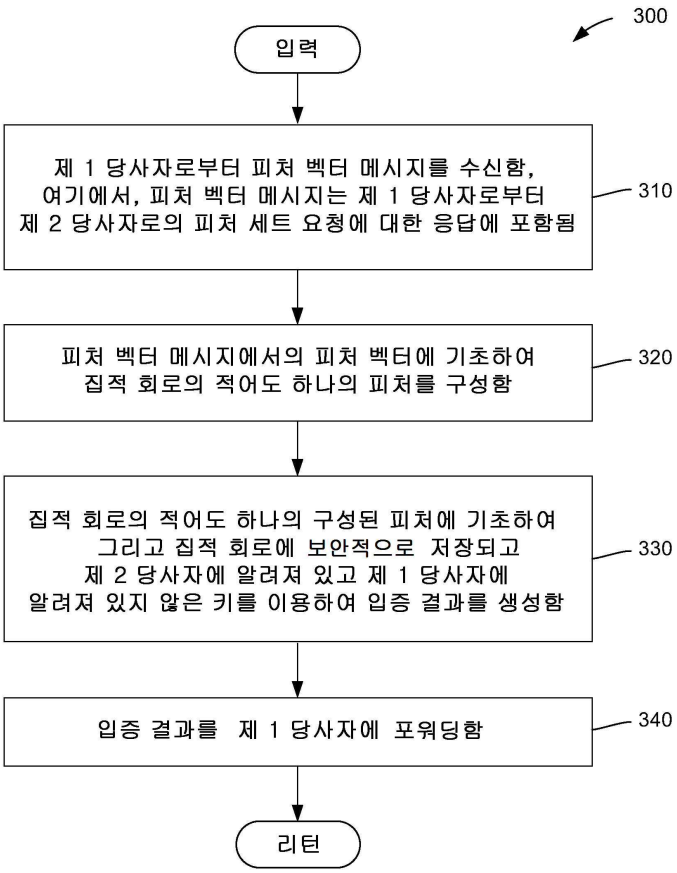
도면1



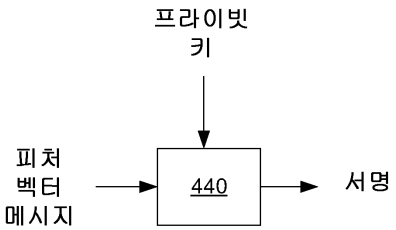
도면2


200
SOC 디바이스
(IC)
210
OTP MEM
240
HWC
250
K
ID #
제 1 당사자
(OEM)
220
제 2 당사자
(공급자)
230
Ks
ID #s
피처 세트 REQ
단계 260
피처 벡터 MSG
단계 264
피처 벡터 MSG
단계 268
MSG
검증
단계 272
피처들
구성
단계 276
입증 결과 생성
단계 280
입증 결과
단계 284
통지 MSG
(시리얼 #. A.
결과,피처 세트)
단계 288
A. 결과 검증
단계 292
확인 MSG
단계 296

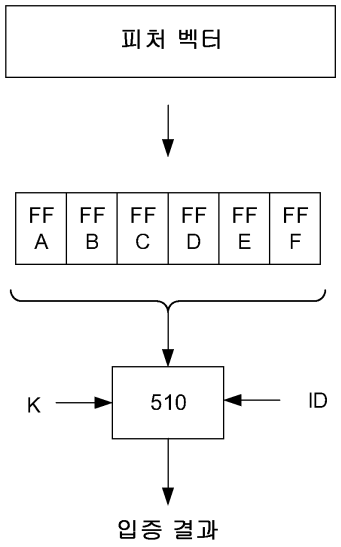
도면3


300
입력
제 1 당사자로부터 피처 벡터 메시지를 수신함,
여기에서, 피처 벡터 메시지는 제 1 당사자로부터
제 2 당사자로의 피처 세트 요청에 대한 응답에 포함됨
310
피처 벡터 메시지에서의 피처 벡터에 기초하여
집적 회로의 적어도 하나의 피처를 구성함
320
집적 회로의 적어도 하나의 구성된 피처에 기초하여
그리고 집적 회로에 보안적으로 저장되고
제 2 당사자에 알려져 있고 제 1 당사자에
알려져 있지 않은 키를 이용하여 입증 결과를 생성함
330
입증 결과를 제 1 당사자에 포워딩함
340
리턴

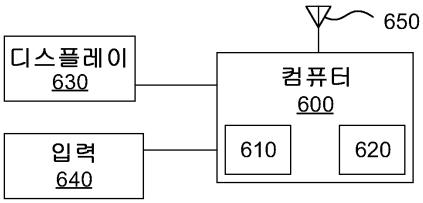
도면4


프라이빗
키
피처
벡터
메시지
440
서명

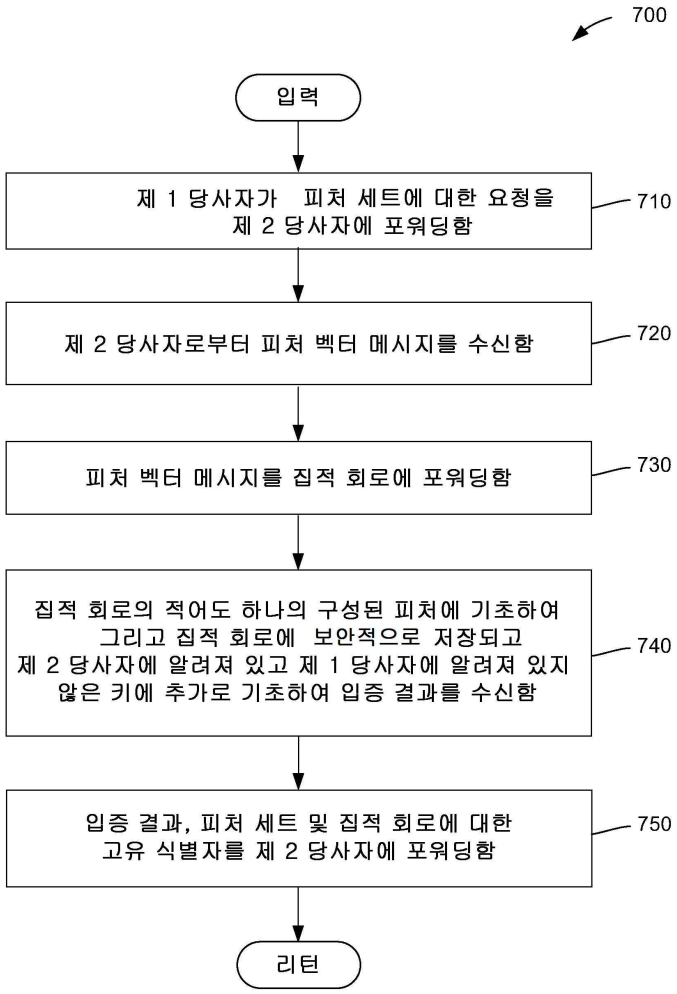
도면5


피처 벡터
FF A
FF B
FF C
FF D
FF E
FF F
K
510
ID
입증 결과

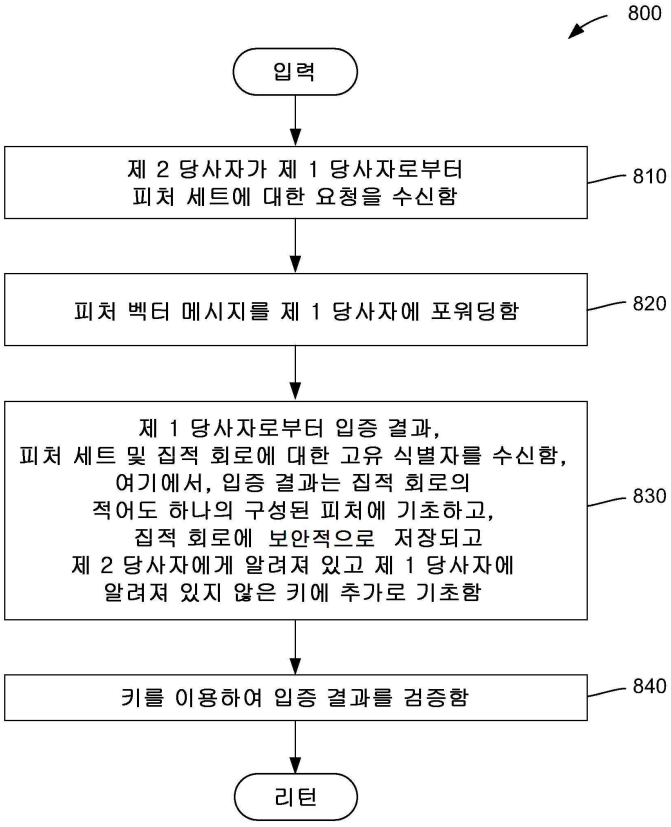
도면6


650
디스플레이
630
컴퓨터
600
610
620
입력
640

도면7


700
입력
제 1 당사자가 피처 세트에 대한 요청을 제 2 당사자에 포워딩함
710
제 2 당사자로부터 피처 벡터 메시지를 수신함
720
피처 벡터 메시지를 집적 회로에 포워딩함
730
집적 회로의 적어도 하나의 구성된 피처에 기초하여 그리고 집적 회로에 보안적으로 저장되고 제 2 당사자에 알려져 있고 제 1 당사자에 알려져 있지 않은 키에 추가로 기초하여 입증 결과를 수신함
740
입증 결과, 피처 세트 및 집적 회로에 대한 고유 식별자를 제 2 당사자에 포워딩함
750
리턴

도면8


800
입력
제 2 당사자가 제 1 당사자로부터
피처 세트에 대한 요청을 수신함
810
피처 벡터 메시지를 제 1 당사자에 포워딩함
820
제 1 당사자로부터 입증 결과,
피처 세트 및 집적 회로에 대한 고유 식별자를 수신함,
여기에서, 입증 결과는 집적 회로의
적어도 하나의 구성된 피처에 기초하고,
집적 회로에 보안적으로 저장되고
제 2 당사자에게 알려져 있고 제 1 당사자에
알려져 있지 않은 키에 추가로 기초함
830
키를 이용하여 입증 결과를 검증함
840
리턴