(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2015-0036423
(43) 공개일자 2015년04월07일

(51) 국제특허분류(Int. Cl.)
G06F 21/62 (2013.01) *G06F 21/72* (2013.01)
G06F 21/87 (2013.01)
(52) CPC특허분류
G06F 21/62 (2013.01)
G06F 21/72 (2013.01)
(21) 출원번호 10-2015-7003202
(22) 출원일자(국제) 2013년07월09일
심사청구일자 없음
(85) 번역문제출일자 2015년02월05일
(86) 국제출원번호 PCT/US2013/049795
(87) 국제공개번호 WO 2014/011687
국제공개일자 2014년01월16일
(30) 우선권주장
61/671,290 2012년07월13일 미국(US)
13/931,708 2013년06월28일 미국(US)

(71) 출원인
퀄컴 인코포레이티드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
바티아, 니라즈
미국 92121 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
오'도노휴, 제레미
미국 92121 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(74) 대리인
특허법인 남앤드남

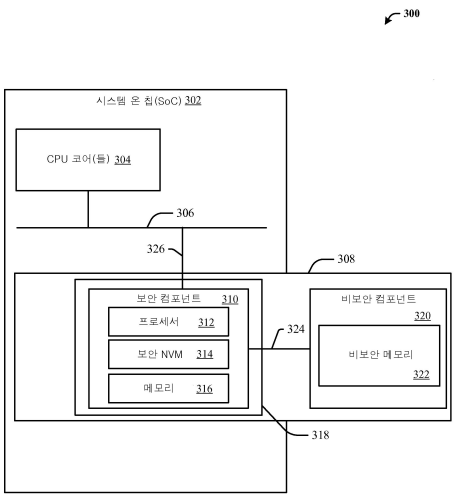
전체 청구항 수 : 총 40 항

(54) 발명의 명칭 **시스템 온 칩 상에 보안 엘리먼트 컴포넌트들의 일부를 통합하기 위한 방법들 및 장치들**

(57) 요 약

효율적인 SE 기능의 제공과 관련하여 무선 통신을 위한 방법, 장치 및 컴퓨터 프로그램 물건이 제공된다. 일례로, 통신 디바이스는 프로세서, RAM 및 NVM, 그리고 보안 컴포넌트 및 비보안 컴포넌트를 포함하는 SE를 포함한다. SE는, SE에 저장된 정보를 통해 액세스 가능한 기능에 액세스하기 위한 요청을 수신하고, 보안 컴포넌트에 저장된, 기능과 연관된 정보의 제 1 부분을 리트리브하고, 비보안 컴포넌트에 저장된, 기능과 연관된 정보의 제 2 부분을 획득하고, 그리고 정보의 획득된 제 2 부분에 대한 액세스를 가능하게 하기 위해 정보의 리트리브된 제 1 부분을 사용하여 기능에 대한 액세스를 가능하게 하는 능력이 있을 수 있다. 한 양상에서, 보안 컴포넌트는 프로세서 및 RAM을 포함할 수 있고, 비보안 컴포넌트는 NVM의 실질적인 전부를 포함할 수 있다.

대 표 도 - 도3



(52) CPC특허분류
G06F 21/87 (2013.01)

명 세 서

청구범위

청구항 1

통신들을 위한 장치로서,

프로세서, 랜덤 액세스 메모리(RAM: random access memory) 및 비휘발성 메모리(NVM: non-volatile memory)를 포함하는 보안 엘리먼트(SE: secure element)를 포함하며,

상기 SE는 상기 SE의 보안 컴포넌트, 상기 SE의 비보안 컴포넌트를 더 포함하고,

상기 비보안 컴포넌트와 상기 보안 컴포넌트는 인터페이스를 통해 커플링되며,

상기 SE는,

상기 SE에 저장된 정보를 통해 액세스 가능한 기능에 액세스하기 위한 요청을 수신하고;

상기 SE의 보안 컴포넌트에 저장된, 상기 기능과 연관된 상기 정보의 제 1 부분을 리트리브하고 - 상기 보안 컴포넌트는 상기 프로세서 및 상기 RAM을 포함함 -;

상기 SE의 비보안 컴포넌트에 저장된, 상기 기능과 연관된 상기 정보의 제 2 부분을 획득하고 - 상기 비보안 컴포넌트는 상기 NVM의 실질적인 전부를 포함함 -; 그리고

상기 정보의 획득된 제 2 부분에 대한 액세스를 가능하게 하기 위해 상기 정보의 리트리브된 제 1 부분을 사용하여 상기 기능에 대한 액세스를 가능하게 하도록 구성되는,

통신들을 위한 장치.

청구항 2

제 1 항에 있어서,

상기 기능은 통신 디바이스에 저장된 애플리케이션이고,

상기 요청은 상기 SE와 상기 통신 디바이스 사이의 암호화에 의한 보안 인터페이스를 통해 수신되는,

통신들을 위한 장치.

청구항 3

제 1 항에 있어서,

상기 SE의 비보안 컴포넌트에 포함된 NVM는 표준 NVM을 포함하는,

통신들을 위한 장치.

청구항 4

제 1 항에 있어서,

상기 SE의 보안 컴포넌트는 보안성 차폐를 사용하여 보안이 확보되는,

통신들을 위한 장치.

청구항 5

제 1 항에 있어서,

상기 SE의 보안 컴포넌트는 시스템 온 칩(SoC: system on chip)에 통합되는,

통신들을 위한 장치.

청구항 6

제 5 항에 있어서,

상기 SoC는 근접장 통신 제어기(NFCC: near field communication controller)인,

통신들을 위한 장치.

청구항 7

제 5 항에 있어서,

상기 SoC는 이동국 모뎀(MSM: mobile station modem) 칩인,

통신들을 위한 장치.

청구항 8

제 5 항에 있어서,

상기 SE의 보안 컴포넌트만을 상기 SoC에 통합함으로써 상기 SoC 상에서 상기 SE의 풋프린트가 최소화되는,

통신들을 위한 장치.

청구항 9

제 8 항에 있어서,

상기 SE의 보안 컴포넌트는 65㎚보다 작거나 같은 기하학적 구조를 갖는,

통신들을 위한 장치.

청구항 10

제 5 항에 있어서,

상기 보안 컴포넌트에 대한 보안성 차폐는 상기 SoC와 연관된 하나 또는 그보다 많은 기존 금속층들을 포함하는,

통신들을 위한 장치.

청구항 11

제 1 항에 있어서,

상기 SE는 상기 SE의 비보안 컴포넌트와 상기 SE의 보안 컴포넌트 사이의 고속 인터페이스를 사용하도록 추가로 구성되는,

통신들을 위한 장치.

청구항 12

제 1 항에 있어서,

상기 SE의 비보안 컴포넌트에 저장된, 상기 기능과 연관된 상기 정보의 제 2 부분은 상기 보안 컴포넌트에 저장된, 상기 기능과 연관된 상기 정보의 제 1 부분을 기초로 암호화된 포맷으로 저장되는,

통신들을 위한 장치.

청구항 13

제 12 항에 있어서,

상기 SE는 상기 정보의 제 1 부분에 포함된 하나 또는 그보다 많은 암호들을 기초로, 상기 SE의 보안 컴포넌트에 포함된 프로세서를 사용하여 상기 정보의 제 2 부분을 복호화하도록 추가로 구성되는,

통신들을 위한 장치.

청구항 14

보안 엘리먼트(SE)를 이용한 통신 방법으로서,

상기 SE에 저장된 정보를 통해 액세스 가능한 기능에 액세스하기 위한 요청을 수신하는 단계 - 상기 SE는 프로세서, 랜덤 액세스 메모리(RAM) 및 비휘발성 메모리(NVM)를 포함함 -;

상기 SE의 보안 컴포넌트에 저장된, 상기 기능과 연관된 상기 정보의 제 1 부분을 리트리브하는 단계 - 상기 보안 컴포넌트는 상기 프로세서 및 상기 RAM을 포함함 -;

상기 SE의 비보안 컴포넌트에 저장된, 상기 기능과 연관된 상기 정보의 제 2 부분을 획득하는 단계 - 상기 비보안 컴포넌트는 상기 NVM의 실질적인 전부를 포함함 -; 및

상기 정보의 획득된 제 2 부분에 대한 액세스를 가능하게 하기 위해 상기 정보의 리트리브된 제 1 부분을 사용하여 상기 기능에 대한 액세스를 가능하게 하는 단계를 포함하는,

보안 엘리먼트(SE)를 이용한 통신 방법.

청구항 15

제 14 항에 있어서,

상기 기능은 통신 디바이스에 저장된 애플리케이션이고,

상기 요청은 상기 SE와 상기 통신 디바이스 사이의 암호화에 의한 보안 인터페이스를 통해 수신되는,

보안 엘리먼트(SE)를 이용한 통신 방법.

청구항 16

제 14 항에 있어서,

상기 SE의 비보안 컴포넌트에 포함된 NVM는 표준 NVM을 포함하는,

보안 엘리먼트(SE)를 이용한 통신 방법.

청구항 17

제 14 항에 있어서,

상기 SE의 보안 컴포넌트는 보안성 차폐를 사용하여 보안이 확보되는,

보안 엘리먼트(SE)를 이용한 통신 방법.

청구항 18

제 14 항에 있어서,

상기 SE의 보안 컴포넌트는 시스템 온 칩(SoC)에 통합되는,

보안 엘리먼트(SE)를 이용한 통신 방법.

청구항 19

제 18 항에 있어서,

상기 SoC는 근접장 통신 제어기(NFCC)인,

보안 엘리먼트(SE)를 이용한 통신 방법.

청구항 20

제 18 항에 있어서,

상기 SoC는 이동국 모뎀(MSM) 칩인,

보안 엘리먼트(SE)를 이용한 통신 방법.

청구항 21

제 18 항에 있어서,

상기 SE의 보안 컴포넌트만을 상기 SoC에 통합함으로써 상기 SoC 상에서 상기 SE의 풋프린트가 최소화되는,

보안 엘리먼트(SE)를 이용한 통신 방법.

청구항 22

제 21 항에 있어서,

상기 SE의 보안 컴포넌트는 65㎚보다 작거나 같은 기하학적 구조를 갖는,

보안 엘리먼트(SE)를 이용한 통신 방법.

청구항 23

제 18 항에 있어서,

상기 보안 컴포넌트에 대한 보안성 차폐는 상기 SoC와 연관된 하나 또는 그보다 많은 기존 금속층들을 포함하는,

보안 엘리먼트(SE)를 이용한 통신 방법.

청구항 24

제 14 항에 있어서,

상기 획득하는 단계는, 상기 SE의 비보안 컴포넌트와 상기 SE의 보안 컴포넌트 사이의 고속 인터페이스를 사용하는 단계를 포함하는,

보안 엘리먼트(SE)를 이용한 통신 방법.

청구항 25

제 14 항에 있어서,

상기 SE의 비보안 컴포넌트에 저장된, 상기 기능과 연관된 상기 정보의 제 2 부분은 상기 보안 컴포넌트에 저장된, 상기 기능과 연관된 상기 정보의 제 1 부분을 기초로 암호화된 포맷으로 저장되는,

보안 엘리먼트(SE)를 이용한 통신 방법.

청구항 26

제 25 항에 있어서,

상기 액세스를 가능하게 하는 단계는, 상기 정보의 제 1 부분에 포함된 하나 또는 그보다 많은 암호들을 기초로, 상기 SE의 보안 컴포넌트에 포함된 프로세서에 의해 상기 정보의 제 2 부분을 복호화하는 단계를 더 포함하는,

보안 엘리먼트(SE)를 이용한 통신 방법.

청구항 27

통신들을 위한 장치로서,

보안 엘리먼트(SE)에 저장된 정보를 통해 액세스 가능한 기능에 액세스하기 위한 요청을 수신하기 위한 수단 - 상기 SE는 프로세서, 랜덤 액세스 메모리(RAM) 및 비휘발성 메모리(NVM)를 포함함 -;

상기 SE의 보안 컴포넌트에 저장된, 상기 기능과 연관된 상기 정보의 제 1 부분을 리트리브하기 위한 수단 -

상기 보안 컴포넌트는 상기 프로세서 및 상기 RAM을 포함함 -;

상기 SE의 비보안 컴포넌트에 저장된, 상기 기능과 연관된 상기 정보의 제 2 부분을 획득하기 위한 수단 - 상기 비보안 컴포넌트는 상기 NVM의 실질적인 전부를 포함함 -; 및

상기 정보의 획득된 제 2 부분에 대한 액세스를 가능하게 하기 위해 상기 정보의 리트리브된 제 1 부분을 사용하여 상기 기능에 대한 액세스를 가능하게 하기 위한 수단을 포함하는,

통신들을 위한 장치.

청구항 28

제 27 항에 있어서,

상기 기능은 통신 디바이스에 저장된 애플리케이션이고,

상기 요청은 상기 SE와 상기 통신 디바이스 사이의 암호화에 의한 보안 인터페이스를 통해 수신되는,

통신들을 위한 장치.

청구항 29

제 27 항에 있어서,

상기 SE의 비보안 컴포넌트에 포함된 NVM는 표준 NVM을 포함하는,

통신들을 위한 장치.

청구항 30

제 27 항에 있어서,

상기 SE의 보안 컴포넌트는 보안성 차폐를 사용하여 보안이 확보되는,

통신들을 위한 장치.

청구항 31

제 27 항에 있어서,

상기 SE의 보안 컴포넌트는 시스템 온 칩(SoC)에 통합되는,

통신들을 위한 장치.

청구항 32

제 31 항에 있어서,

상기 SoC는 근접장 통신 제어기(NFCC)인,

통신들을 위한 장치.

청구항 33

제 31 항에 있어서,

상기 SoC는 이동국 모뎀(MSM) 칩인,

통신들을 위한 장치.

청구항 34

제 31 항에 있어서,

상기 SE의 보안 컴포넌트만을 상기 SoC에 통합함으로써 상기 SoC 상에서 상기 SE의 풋프린트가 최소화되는,

통신들을 위한 장치.

청구항 35

제 34 항에 있어서,

상기 SE의 보안 컴포넌트는 65㎚보다 작거나 같은 기하학적 구조를 갖는,

통신들을 위한 장치.

청구항 36

제 31 항에 있어서,

상기 보안 컴포넌트에 대한 보안성 차폐는 상기 SoC와 연관된 하나 또는 그보다 많은 기존 금속층들을 포함하는,

통신들을 위한 장치.

청구항 37

제 36 항에 있어서,

상기 획득하기 위한 수단은, 상기 SE의 비보안 컴포넌트와 상기 SE의 보안 컴포넌트 사이의 고속 인터페이스를 사용하도록 추가로 구성되는,

통신들을 위한 장치.

청구항 38

제 27 항에 있어서,

상기 SE의 비보안 컴포넌트에 저장된, 상기 기능과 연관된 상기 정보의 제 2 부분은 상기 보안 컴포넌트에 저장된, 상기 기능과 연관된 상기 정보의 제 1 부분을 기초로 암호화된 포맷으로 저장되는,

통신들을 위한 장치.

청구항 39

제 38 항에 있어서,

상기 액세스를 가능하게 하기 위한 수단은, 상기 정보의 제 1 부분에 포함된 하나 또는 그보다 많은 암호들을 기초로, 상기 정보의 제 2 부분을 복호화하도록 추가로 구성되는,

통신들을 위한 장치.

청구항 40

컴퓨터 프로그램 물건으로서,

보안 엘리먼트(SE)에 저장된 정보를 통해 액세스 가능한 기능에 액세스하기 위한 요청을 수신하기 위한 코드 － 상기 SE는 프로세서, 랜덤 액세스 메모리(RAM) 및 비휘발성 메모리(NVM)를 포함함 －;

상기 SE의 보안 컴포넌트에 저장된, 상기 기능과 연관된 상기 정보의 제 1 부분을 리트리브하기 위한 코드 － 상기 보안 컴포넌트는 상기 프로세서 및 상기 RAM을 포함함 －;

상기 SE의 비보안 컴포넌트에 저장된, 상기 기능과 연관된 상기 정보의 제 2 부분을 획득하기 위한 코드 － 상기 비보안 컴포넌트는 상기 NVM의 실질적인 전부를 포함함 －; 및

상기 정보의 획득된 제 2 부분에 대한 액세스를 가능하게 하기 위해 상기 정보의 리트리브된 제 1 부분을 사용하여 상기 기능에 대한 액세스를 가능하게 하기 위한 코드를 포함하는,

컴퓨터 판독 가능 매체를 포함하는,

컴퓨터 프로그램 물건.

발명의 설명

기 술 분 야

[0001] 본 특허출원은 "METHODS AND APPARATUSES FOR INTEGRATING A PORTION OF SECURE ELEMENT COMPONENTS ON A SYSTEM ON CHIP"이라는 명칭으로 2012년 7월 13일자 출원된 가출원 제61/671,290호에 대한 우선권을 주장하며, 이 가출원은 본 출원의 양수인에게 양도되었고 이로써 인용에 의해 본 명세서에 명백히 포함된다.

[0002] 개시된 양상들은 일반적으로 디바이스들 간의 그리고/또는 디바이스들 내에서의 통신들에 관한 것으로, 구체적으로는 보안 엘리먼트의 일부분이 시스템 온 칩(SoC: system on chip)에 통합되는 보안 엘리먼트들을 사용하기 위한 방법들 및 시스템들에 관한 것이다.

배 경 기 술

[0003] 기술의 발전들은 더 작고 더 강력한 개인용 컴퓨팅 디바이스들을 창출해 왔다. 예를 들어, 각각 작고 가벼우며 사용자들이 쉽게 휴대할 수 있는 휴대용 무선 전화들, 개인용 디지털 보조기기(PDA: personal digital assistant)들 및 페이징 디바이스들과 같은 무선 컴퓨팅 디바이스들을 비롯하여, 현재 다양한 휴대용 개인 컴퓨팅 디바이스들이 존재한다. 보다 구체적으로, 예를 들어 휴대용 무선 전화들은 무선 네트워크들을 통해 음성 및 데이터 패킷들을 전달하는 셀룰러 전화들을 더 포함한다. 이러한 많은 셀룰러 전화들은 컴퓨팅 능력들에 있어 비교적 큰 증가들을 갖도록 제조되고 있으며, 그에 따라 소형 개인용 컴퓨터들 및 핸드헬드 PDA들과 동등해지고 있다. 또한, 이러한 디바이스들은 다양한 주파수들 및 적용 가능한 커버리지 영역들을 사용하는 통신들, 예컨대 셀룰러 통신들, 무선 근거리 네트워크(WLAN: wireless local area network) 통신들, 근접장 통신(NFC: near field communication) 등을 가능하게 하도록 제조되고 있다.

[0004] 현재, 디바이스 내에서 일부 애플리케이션들은 물리적 그리고/또는 소프트웨어 침입들에 대한 보호를 포함하는 높은 레벨들의 보안을 사용하도록 구성될 수 있다. 이러한 애플리케이션들은 보안 엘리먼트(SE: secure element)들에서 호스팅될 수 있다. 본 명세서에서 사용되는 바와 같이, SE는 무단 액세스를 막도록 강화된 완벽한 컴퓨팅 플랫폼(예를 들어, 랜덤 액세스 메모리(RAM: random access memory), 판독 전용 메모리(ROM: read only memory), 비휘발성 메모리(NVM: non-volatile memory), 암호화 가속기들, 중앙 처리 유닛(CPU: central processing unit) 등)을 포함할 수 있다. 이러한 SE들은 매우 높은 레벨들의 보안성을 달성할 수 있지만, 이들은 또한 디바이스에 통합될 때 비용이 상대적으로 많이 들 수도 있다. 예를 들어, SE는 일반적으로 별개의 실리콘 프로세스들을 사용하여 생성되며, 이에 따라 통합된 SoC 상에서의 가능한 비용 이익들로부터 이익을 얻지 못할 수도 있다.

[0005] 따라서 효율적인 SE 기능을 제공하기 위한 개선된 방법들 및 장치들이 요구될 수 있다.

발명의 내용

[0006] 다음은 하나 또는 그보다 많은 양상들의 기본적인 이해를 제공하도록 이러한 양상들의 간단한 요약을 제시한다. 이 요약은 고려되는 모든 양상들의 포괄적인 개요가 아니며, 모든 양상들의 주요 또는 핵심 엘리먼트들을 식별하지도, 임의의 또는 모든 양상들의 범위를 기술하지도 않는 것으로 의도된다. 그 유일한 목적은 하나 또는 그보다 많은 양상들의 일부 개념들을 뒤에 제시되는 보다 상세한 설명에 대한 서론으로서 간단한 형태로 제시하는 것이다.

[0007] 하나 또는 그보다 많은 양상들 및 그에 대응하는 개시에 따르면, 효율적인 SE 기능의 제공과 관련하여 다양한 양상들이 설명된다. 일례로, 통신 디바이스는 프로세서, RAM 및 NVM, 보안 컴포넌트 및 비보안 컴포넌트를 포함하는 SE를 포함한다. 한 양상에서, 비보안 컴포넌트와 보안 컴포넌트는 인터페이스를 통해 커플링된다. SE는, SE에 저장된 정보를 통해 액세스 가능한 기능에 액세스하기 위한 요청을 수신하고, SE의 보안 컴포넌트에 저장된, 기능과 연관된 정보의 제 1 부분을 리트리브하고, SE의 비보안 컴포넌트에 저장된, 기능과 연관된 정보의 제 2 부분을 획득하고, 그리고 정보의 획득된 제 2 부분에 대한 액세스를 가능하게 하기 위해 정보의 리트리브된 제 1 부분을 사용하여 기능에 대한 액세스를 가능하게 하는 능력이 있을 수 있다. 한 양상에서, 보안 컴포넌트는 프로세서 및 RAM을 포함할 수 있고, 비보안 컴포넌트는 NVM의 실질적인 전부를 포함할 수 있다.

[0008] 관련된 양상들에 따르면, 효율적인 SE 기능을 제공하기 위한 방법이 제공된다. 상기 방법은 상기 SE에 저장된 정보를 통해 액세스 가능한 기능에 액세스하기 위한 요청을 수신하는 단계를 포함할 수 있다. 한 양상에서, 상기 SE는 프로세서, RAM 및 NVM을 포함할 수 있다. 또한, 상기 방법은 상기 SE의 보안 컴포넌트에 저장된, 상기

기능과 연관된 상기 정보의 제 1 부분을 리트리브하는 단계를 포함할 수 있다. 한 양상에서, 상기 보안 컴포넌트는 프로세서 및 RAM을 포함할 수 있다. 또한, 상기 방법은 상기 SE의 비보안 컴포넌트에 저장된, 상기 기능과 연관된 상기 정보의 제 2 부분을 획득하는 단계를 포함할 수 있다. 한 양상에서, 상기 비보안 컴포넌트는 NVM의 실질적인 전부를 포함할 수 있다. 더욱이, 상기 방법은 상기 정보의 획득된 제 2 부분에 대한 액세스를 가능하게 하기 위해 상기 정보의 리트리브된 제 1 부분을 사용하여 상기 기능에 대한 액세스를 가능하게 하는 단계를 포함할 수도 있다.

[0009] 다른 양상은 효율적인 SE 기능을 제공하는 것이 가능한 통신 장치에 관한 것이다. 상기 통신 장치는 상기 SE에 저장된 정보를 통해 액세스 가능한 기능에 액세스하기 위한 요청을 수신하기 위한 수단을 포함할 수 있다. 한 양상에서, 상기 SE는 프로세서, RAM 및 NVM을 포함할 수 있다. 또한, 상기 통신 장치는 상기 SE의 보안 컴포넌트에 저장된, 상기 기능과 연관된 상기 정보의 제 1 부분을 리트리브하기 위한 수단을 포함할 수 있다. 한 양상에서, 상기 보안 컴포넌트는 프로세서 및 RAM을 포함할 수 있다. 또한, 상기 통신 장치는 상기 SE의 비보안 컴포넌트에 저장된, 상기 기능과 연관된 상기 정보의 제 2 부분을 획득하기 위한 수단을 포함할 수 있다. 한 양상에서, 상기 비보안 컴포넌트는 NVM의 실질적인 전부를 포함할 수 있다. 더욱이, 상기 통신 장치는 상기 정보의 획득된 제 2 부분에 대한 액세스를 가능하게 하기 위해 상기 정보의 리트리브된 제 1 부분을 사용하여 상기 기능에 대한 액세스를 가능하게 하기 위한 수단을 포함할 수 있다.

[0010] 다른 양상은 통신 장치에 관한 것이다. 상기 장치는 SE를 포함할 수 있는데, 상기 SE는 프로세서, RAM 및 NVM, 상기 SE의 보안 컴포넌트 및 상기 SE의 비보안 컴포넌트를 포함한다. 상기 SE는 상기 SE에 저장된 정보를 통해 액세스 가능한 기능에 액세스하기 위한 요청을 수신하도록 구성될 수 있다. 또한, 상기 SE는 상기 SE의 보안 컴포넌트에 저장된, 상기 기능과 연관된 상기 정보의 제 1 부분을 리트리브하도록 구성될 수 있다. 한 양상에서, 상기 보안 컴포넌트는 프로세서 및 RAM을 포함할 수 있다. 또한, 상기 SE는 상기 SE의 비보안 컴포넌트에 저장된, 상기 기능과 연관된 상기 정보의 제 2 부분을 획득하도록 구성될 수 있다. 한 양상에서, 상기 비보안 컴포넌트는 NVM의 실질적인 전부를 포함할 수 있다. 더욱이, 상기 SE는 상기 정보의 획득된 제 2 부분에 대한 액세스를 가능하게 하기 위해 상기 정보의 리트리브된 제 1 부분을 사용하여 상기 기능에 대한 액세스를 가능하게 하도록 구성될 수 있다.

[0011] 또 다른 양상은 컴퓨터 프로그램 물건에 관한 것으로, 이는 SE에 저장된 정보를 통해 액세스 가능한 기능에 액세스하기 위한 요청을 수신하기 위한 코드를 포함하는 컴퓨터 판독 가능 매체를 가질 수 있다. 한 양상에서, 상기 SE는 프로세서, RAM 및 NVM을 포함할 수 있다. 또한, 상기 컴퓨터 판독 가능 매체는 상기 SE의 보안 컴포넌트에 저장된, 상기 기능과 연관된 상기 정보의 제 1 부분을 리트리브하기 위한 코드를 포함할 수 있다. 한 양상에서, 상기 보안 컴포넌트는 프로세서 및 RAM을 포함할 수 있다. 또한, 상기 컴퓨터 판독 가능 매체는 상기 SE의 비보안 컴포넌트에 저장된, 상기 기능과 연관된 상기 정보의 제 2 부분을 획득하기 위한 코드를 포함할 수 있다. 한 양상에서, 상기 비보안 컴포넌트는 NVM의 실질적인 전부를 포함할 수 있다. 더욱이, 상기 컴퓨터 판독 가능 매체는 상기 정보의 획득된 제 2 부분에 대한 액세스를 가능하게 하기 위해 상기 정보의 리트리브된 제 1 부분을 사용하여 상기 기능에 대한 액세스를 가능하게 하기 위한 코드를 포함할 수 있다.

[0012] 앞서 언급된 그리고 관련된 목적들의 이행을 위해, 하나 또는 그보다 많은 양상들은, 이후에 충분히 설명되며 청구항들에서 특별히 지적되는 특징들을 포함한다. 다음 설명 및 첨부 도면들은 하나 또는 그보다 많은 양상들의 특정 예시적인 특징들을 상세히 설명한다. 그러나 이러한 특징들은 다양한 양상들의 원리들이 채용될 수 있는 다양한 방식들 중 몇몇을 나타낼 뿐이며, 이러한 설명은 이러한 모든 양상들 및 그 등가물들을 포함하는 것으로 의도된다.

도면의 간단한 설명

[0013] 개시되는 양상들은 이하, 개시되는 양상들을 한정하는 것이 아니라 예시하기 위해 제공되는 첨부 도면들과 함께 설명될 것이며, 여기서 동일 부호들은 동일 엘리먼트들을 나타낸다.

도 1은 한 양상에 따른 유도 기반 통신 시스템의 단순화된 블록도이다.

도 2는 한 양상에 따른 유도 기반 시스템의 단순화된 개략도이다.

도 3은 한 양상에 따른, 통합된 SE를 갖는 SoC의 블록도이다.

도 4는 한 양상에 따라, SoC에 통합된 SE를 사용하기 위한 예시적인 방법을 설명하는 흐름도이다.

도 5는 본 개시에 따른 통신 디바이스의 양상들의 블록도이다.

도 6은 한 양상에 따라, 효율적인 SE 기능을 제공하기 위한 통신 디바이스의 일례의 블록도를 나타낸다.

발명을 실시하기 위한 구체적인 내용

[0014] 이제, 도면들을 참조하여 다양한 양상들이 설명된다. 다음 설명에서는, 하나 또는 그보다 많은 양상들의 철저한 이해를 제공하기 위해, 설명을 목적으로 다수의 특정 세부사항들이 제시된다. 그러나 이러한 특정 세부사항들 없이 이러한 양상(들)이 실시될 수도 있음이 명백할 수 있다.

[0015] 일반적으로, 통신 디바이스는 SE의 사용을 통해 다양한 기능들에 액세스할 수 있다. SE는 일반적으로 무단 액세스를 막도록 강화된 정보를 저장하기 위한 환경을 제공한다. 또한, SE는 RAM, ROM, NV 메모리(NVM), 암호화 가속기들, CPU 등과 같은, 그러나 이에 한정된 것은 아닌 다양한 컴포넌트들을 포함할 수 있다. 본 명세서에서 설명되는 바와 같이, SoC에서 SE의 컴포넌트들 중 하나 또는 그보다 많은 컴포넌트가 분리되어 포함(예를 들어, 통합)될 수 있는 시스템 아키텍처가 제시된다. 이에 따라, 통합된 그리고 더 낮은 비용의 아키텍처를 사용하여 종래의 모놀리식(monolithic) SE 설계들과 비슷한 레벨들의 보안이 달성될 수 있다.

[0016] 도 1은 본 발명의 다양한 예시적인 실시예들에 따른 유도 기반 통신 시스템(100)을 나타낸다. 에너지 전달을 제공하기 위한 방사 필드(radiated field)(106)를 발생시키기 위해 송신기(104)에 입력 전력(102)이 제공된다. 수신기(108)는 방사 필드(106)에 커플링하고, 출력 전력(110)에 커플링된 (도시되지 않은) 디바이스에 의한 저장 또는 소비를 위한 출력 전력(110)을 발생시킨다. 송신기(104)와 수신기(108) 모두 거리(112)를 두고 분리된다. 한 예시적인 실시예에서, 송신기(104)와 수신기(108)는 상호 공진 관계에 따라 구성되고, 수신기(108)의 공진 주파수와 송신기(104)의 공진 주파수가 매우 가까울 때, 송신기(104)와 수신기(108) 사이의 전송 손실들은, 수신기(108)가 방사 필드(106)의 "근접장"에 로케이팅되는 경우에 최소가 된다.

[0017] 송신기(104)는 에너지 송신을 위한 수단을 제공하기 위한 송신 안테나(114)를 더 포함하고, 수신기(108)는 에너지 수신을 위한 수단을 제공하기 위한 수신 안테나(118)를 더 포함한다. 송신 및 수신 안테나들은 애플리케이션들 및 이들과 연관될 디바이스들에 따라 크기가 정해진다. 명시된 바와 같이, 전자기파의 에너지의 대부분을 원거리장(far field)으로 전파하기보다는, 송신 안테나의 근접장의 에너지의 상당 부분을 수신 안테나에 커플링함으로써 효율적인 에너지 전달이 일어난다. 이러한 근접장에 있을 때, 송신 안테나(114)와 수신 안테나(118) 사이에 커플링 모드가 전개될 수 있다. 이러한 근접장 커플링이 일어날 수 있는 안테나들(114, 118) 주위의 영역은 본 명세서에서 커플링 모드 구역으로 지칭된다.

[0018] 도 2는 근접장 유도 기반 통신 시스템의 단순화된 개략도를 보여준다. 송신기(204)는 발진기(222), 전력 증폭기(224) 그리고 필터 및 정합 회로(226)를 포함한다. 발진기(222)는 조절 신호(223)에 응답하여 조정될 수 있는 원하는 주파수로 신호를 발생시키도록 구성된다. 발진기 신호는 제어 신호(225)에 응답하는 증폭량으로 전력 증폭기(224)에 의해 증폭될 수 있다. 필터 및 정합 회로(226)는 고조파들 또는 다른 원치 않는 주파수들을 필터링하고 송신기(204)의 임피던스를 송신 안테나(214)에 정합시키기 위해 포함될 수 있다.

[0019] 수신기(208)는 정합 회로(232) 그리고 정류기 및 스위칭 회로(234)를 포함하여, 도 2에 도시된 바와 같이 배터리(236)를 충전하거나 수신기에 커플링된 디바이스(도시되지 않음)에 전력을 공급하기 위한 DC 전력 출력을 발생시킬 수 있다. 정합 회로(232)는 수신기(208)의 임피던스를 수신 안테나(218)에 정합시키기 위해 포함될 수 있다. 수신기(208) 및 송신기(204)는 개별 통신 채널(219)(예를 들어, 블루투스, 지그비(Zigbee), 셀룰러 등)을 통해 통신할 수 있다.

[0020] 도 3을 참조하면, 한 양상에 따른 NFC 시스템 아키텍처(300)의 블록도가 예시된다. NFC 시스템 아키텍처(300)는 공유 버스(306)의 사용을 통해 하나 또는 그보다 많은 CPU 코어들(304)에 대한 처리를 가능하게 하도록 구성될 수 있는 SoC(302)를 포함할 수 있다. 한 양상에서, SoC(302)는 이동국 모뎀(MSM: mobile station modem) 칩을 나타낼 수 있다. 다른 양상에서, SoC(302)는 NFC 제어기(NFCC: NFC controller)를 나타낼 수도 있다.

[0021] NFC 시스템 아키텍처(300)는 추가로 SE(308)를 포함한다. 한 양상에서, SE(308)는 가입자 식별 모듈(SIM: subscriber identification module) 카드, 보안 디지털(SD: secure digital) 카드, 마이크로 SD 카드 및/또는 임베디드 SE(308)일 수 있다. SE(308)는 보안 컴포넌트(310) 및 비보안 컴포넌트(320)를 포함할 수 있다. 보안 컴포넌트(310)와 비보안 컴포넌트(320)는 인터페이스(324)를 통해 커플링될 수 있다. 한 양상에서, 인터페이스(324)는 암호화를 지원하는 버스 인터페이스를 사용하도록 구성될 수 있다. 다른 양상에서, 인터페이스(324)는 표준 고속 인터페이스일 수도 있다. 이러한 양상에서, 인터페이스(324)는 처리를 위해 SE(308)의 비보안 메모리(322)로부터 보안 컴포넌트(310)로의 코드, 애플릿들 등의 효율적인 로딩을 제공한다.

[0022] 보안 컴포넌트(310)는 프로세서(312), 보안 NVM(314) 및 메모리(316)를 포함할 수 있다. 한 양상에서, 프로세서(312)는 SE(308)와 연관된 전용 프로세서(312)일 수 있다. 다른 양상에서, 프로세서(312)는 SE(308) 내에서 보안성 및 무결성을 유지하는데 도움이 되도록 SoC(302)를 통해 추가적인 보안 보호들(예를 들어, 암호화, 서명들 등)에 이용 가능한 프로세서일 수도 있다. 한 양상에서, 보안 NVM(314)은 보호(예를 들어, 루트 키들, 인증서들 등)로부터 이익을 얻을 수 있는 다양한 아이템들을 저장하기에 충분한 메모리를 포함할 수 있다. 한 양상에서, 메모리(316)는 비보안 메모리(322)에 저장된 정보의 효율적인 로딩 및 처리를 가능하게 하기에 충분한 저장 능력을 포함할 수 있다.

[0023] 또한, 보안 컴포넌트(310)는 보안성 차폐(318)를 사용하여 보안이 확보될 수 있다. 한 양상에서, 보안성 차폐(318)는 하드웨어 및/또는 소프트웨어 공격들에 대한 다양한 예방책들(예를 들어, 차동 전력 분석(DPA: differential power analysis), 단순 전력 분석(SPA: simple power analysis), 레이저 공격들, 전압 변화들, 온도 변화들, 레이저 프로빙(probing) 등)을 제공할 수 있다. 보안성 차폐(318) 예방책들은 내부 동작의 관찰을 더 어렵게 하는 금속층들, 패키지가 열리면 동작을 불가능하게 하는 광 센서들, 유사한 동작들에 대한 다수의 하드웨어 경로들 등을 포함할 수 있지만, 이들에 한정된 것은 아니다. 한 양상에서, 보안성 차폐(318)는 SoC(302)와 연관된 기존 금속층들을 사용하여 보안성 차폐 형태들에 대한 디지털 또는 아날로그 IP를 구현할 수 있다.

[0024] 비보안 컴포넌트(320)는 비보안 메모리(322)를 포함할 수 있다. 한 양상에서, 비보안 메모리(322)는 보안 저장소, 표준 NVM, RAM, 임의의 메모리 저장 디바이스, 또는 이들의 임의의 결합을 제공하는 작업으로 특수화될 수 있다. 한 양상에서, 비보안 메모리(322)는 대략 1.2Mbytes의 공간으로 구성될 수 있다. 다른 양상에서, 비보안 메모리(322)는 SE(308)를 통해 액세스 가능한 다양한 기능들과 연관된 코드, 애플릿들 등을 저장하는데 사용될 수도 있다. 이러한 양상에서, 비보안 메모리(322)는 애플리케이션들(예를 들어, 컴퓨터 코드) 및 데이터의 비휘발성 저장소로 사용될 수 있고, 보안 NVM(314)은 애플리케이션들과 연관된 키 시스템을 저장하는데 사용될 수 있다. 한 양상에서는, 외부 인터페이스를 통한 공격들에 대해 코드 및 데이터의 보안성 및 무결성을 유지하는데 도움이 되도록, 데이터가 SoC(302)를 떠날 때마다 데이터가 (보안을 확보하도록) 암호화되고 (무결성을 보장하도록) 서명될 수 있다. 이에 따라, 비보안 메모리(322) 내의 정보는 보안 컴포넌트(310) 내에서 사용되는 암호화 연산들에 의해 제공되는 능력 범위까지 보안이 확보될 수 있다.

[0025] 동작 양상에서, SE(308)는 '공통 평가 기준(Common Criteria)'으로 알려진 지침들에 따라 안전한 것으로 인증될 수 있다. 이러한 지침들은, 내부에서 보안이 평가되도록 정의되는 평가 대상(TOE: Target of Evaluation)을 평가한다. 도 3에 도시된 바와 같이, 보안 컴포넌트(310) 및 비보안 컴포넌트(320)를 포함하는 SE(308)가 TOE로서 평가될 수 있다. 즉, 현재 사용되는 TOE들과 상당히 유사할 수 있는 TOE를 보유하기 위해, 보안 컴포넌트(310)와 SoC(302)의 다른 컴포넌트들 사이의 인터페이스들(326)이 최소화될 수 있다. 이러한 양상에서, 인터페이스들(326)은 특정 eFuse 데이터를 SE(308)에 대해서만 이용 가능해지게 하도록 구성될 수 있다. 다른 양상에서, 인터페이스들(326)은 SoC(302)의 내부(RAM) 메모리에 대해 암호화로 보안이 확보되어, 다른 프로세서들(예를 들어, SoC(302) 내의 CPU 코어들(304))에 의한 SE(308) 동작의 관찰을 막을 수 있다. 다른 양상에서, 보안 컴포넌트(310)는 SoC(302) 상의 다른 컴포넌트들(예를 들어, 304)과 분리된 전력 도메인들 및/또는 전력 관리를 사용할 수 있다. 또 다른 양상에서, 보안 컴포넌트(310)는 예를 들어, 이진 범용 비동기화 수신기/송신기(UART: universal asynchronous receiver/transmitter) 인터페이스를 사용하여 다른 프로세서들(예를 들어, 304)과의 인터페이스들을 제한할 수 있다.

[0026] 따라서 SE(308)의 다양한 기능들이 SoC(302) 상의 소형 실리콘 기하학적 구조들로 효율적으로 구현될 수 있는 보안 컴포넌트(310) 및 더 크고 비용이 더 많이 드는 기하학적 구조들 상에 더 효율적으로 구현될 수 있는 비보안 컴포넌트(320)로 나뉠 수 있는 NFC 시스템 아키텍처(300)가 제시된다.

[0027] 도 4는 제시된 대상의 다양한 양상들에 따른 다양한 방법들을 나타낸다. 설명의 단순화를 위해, 방법들은 일련의 동작들 또는 시퀀스 단계들로서 도시 및 설명되지만, 일부 동작들은 본 명세서에서 도시 및 설명되는 것과 다른 순서들로 그리고/또는 다른 동작들과 동시에 일어날 수 있으므로, 청구 대상은 동작들의 순서로 한정되지는 않는다고 이해 및 인식되어야 한다. 예를 들어, 해당 기술분야에서 통상의 지식을 가진 자들은, 방법이 대안적으로 상태도에서와 같이 일련의 상호 관련 상태들이나 이벤트들로서 표현될 수 있다고 이해 및 인식할 것이다. 더욱이, 청구 대상에 따라 방법을 구현하기 위해, 예시되는 모든 동작들이 필요한 것은 아닐 수도 있다. 추가로, 이후에 그리고 본 명세서 전반에 개시되는 방법들은 이러한 방법들을 컴퓨터들로 전송 및 전달하는 것을 가능하게 하기 위한 제조품에 저장될 수 있다고 또한 인식되어야 한다. 본 명세서에서 사용되는 제조품이라는 용어는 임의의 컴퓨터 판독 가능 디바이스, 반송파 또는 매체로부터 액세스 가능한 컴퓨터 프로그램을 포괄

하는 것으로 의도된다.

[0028] 이제 도 4를 참조하면, SoC와 적어도 부분적으로 통합되는 SE를 사용하기 위한 프로세스(400)를 설명하는 예시적인 흐름도가 예시된다. 한 양상에서, 프로세스(400)는 SE(예를 들어, SE(560))를 포함하는 통신 디바이스(예를 들어, 통신 디바이스(500))에 의해 수행될 수 있다.

[0029] 블록(402)에서, SE는 기능(예를 들어, 애플리케이션)에 액세스하기 위한 요청을 수신할 수 있다. 한 양상에서, 요청은 애플리케이션의 활성화, 하나 또는 그보다 많은 센서들로부터 획득된 측정들, 다른 디바이스로부터 수신된 데이터 등에 응답하여 수신될 수 있다. 한 양상에서, 요청은 SE와 통신 디바이스 사이의 암호화에 의한 보안 인터페이스를 통해 수신될 수 있다.

[0030] 블록(404)에서, SE는 SE의 보안 컴포넌트로부터 기능과 연관된 정보의 일부분을 리트리브할 수 있다. 한 양상에서, 정보는 요청된 기능에 안전한 방식으로 액세스하는 것과 연관된 키, 인증서 등을 포함할 수 있다. 다른 양상에서, SE의 보안 컴포넌트는 MSM 칩, NFCC 등과 같은, 그러나 이에 한정된 것은 아닌 SoC에 통합될 수 있다. 한 양상에서, SE의 보안 컴포넌트만을 SoC에 통합함으로써 SoC 상에서 SE의 풋프린트가 최소화될 수 있다. 다른 양상에서, SE의 보안 컴포넌트는 65㎚보다 작거나 같은 기하학적 구조를 가질 수 있다.

[0031] 블록(406)에서, SE는 SE의 비보안 컴포넌트 내의 저장소로부터 기능과 연관된 정보의 일부분을 획득할 수 있다. 한 양상에서, 비보안 컴포넌트는 SE를 통해 액세스 가능한 다양한 기능들과 연관된 코드, 애플릿들 등을 저장할 수 있는 표준 NVM을 포함할 수 있다. 다른 양상에서, 정보의 리트리브된 부분은 고속 인터페이스를 통해 SE의 보안 컴포넌트에 전달될 수 있다. 이러한 양상에서, 리트리브된 부분은 SE의 보안 컴포넌트에서 이용 가능한 메모리에 배치될 수 있다. 한 양상에서, SE의 비보안 컴포넌트에 저장된 정보의 일부는 보안 컴포넌트에 저장된 정보의 일부를 기초로 암호화된 포맷으로 저장될 수 있다.

[0032] 블록(408)에서, SE는 SE의 비보안 컴포넌트로부터 획득된 정보 및 SE의 보안 컴포넌트로부터의 정보를 기초로 기능에 대한 액세스를 가능하게 할 수 있다. SE의 비보안 컴포넌트에 저장된 정보의 일부가 암호화된 포맷으로 저장될 수 있는 한 양상에서, 액세스를 가능하게 하는 것은 정보를 복호화하는 것을 포함할 수 있다.

[0033] 이에 따라, 프로세스(400)는 SoC에 적어도 부분적으로 통합되는 SE를 사용하기 위한 방법을 제공한다.

[0034] 도 3을 참조하지만, 이제 도 5를 또한 참조하면, 통신 디바이스(500)의 예시적인 아키텍처가 예시된다. 도 5에 도시된 바와 같이, 통신 디바이스(500)는 예컨대, (도시되지 않은) 수신 안테나로부터 신호를 수신하고, 수신 신호에 대해 일반적인 동작들을 수행(예를 들어, 필터링, 증폭, 하향 변환 등)하고, 조정된 신호를 디지털화하여 샘플들을 획득하는 수신기(502)를 포함한다. 수신기(502)는 수신된 심벌들을 복조하여 이들을 채널 추정을 위해 프로세서(506)에 제공할 수 있는 복조기(504)를 포함할 수 있다. 프로세서(506)는, 수신기(502)에 의해 수신된 정보의 분석 및/또는 송신기(520)에 의한 송신을 위한 정보의 생성에 전용되는 프로세서, 통신 디바이스(500)의 하나 또는 그보다 많은 컴포넌트들을 제어하는 프로세서, 그리고/또는 수신기(502)에 의해 수신된 정보의 분석, 송신기(520)에 의한 송신을 위한 정보의 생성, 및 통신 디바이스(500)의 하나 또는 그보다 많은 컴포넌트들의 제어 모두를 수행하는 프로세서일 수 있다. 또한, 송신기(520)에 의한 송신을 위해, 프로세서(506)에 의해 처리되는 신호들을 변조할 수 있는 변조기(518)를 통해 신호들이 준비될 수 있다.

[0035] 통신 디바이스(500)는 프로세서(506)에 작동 가능하게 연결되며 전송될 데이터, 수신된 데이터, 이용 가능한 채널들과 관련된 정보, TCP 플로우들, 간섭 세기 및/또는 분석된 신호와 연관된 데이터, 할당된 채널, 전력, 레이트 등과 관련된 정보, 그리고 채널을 추정하고 채널을 통해 통신하기 위한 임의의 다른 적당한 정보를 저장할 수 있는 메모리(508)를 추가로 포함할 수 있다. 또한, 프로세서(506) 및/또는 디바이스 호스트(534)는 NFC 시스템의 제어를 돕도록 구성될 수 있다.

[0036] 한 양상에서, 프로세서(506), NFCC(530) 및/또는 SE(560)는 SE(560)에 저장된 정보를 통해 액세스 가능한 기능에 액세스하기 위한 요청을 수신하기 위한 수단, SE(560)의 보안 컴포넌트(562)에 저장된, 기능과 연관된 정보의 제 1 부분을 리트리브하기 위한 수단, SE(560)의 비보안 컴포넌트(564)에 저장된, 기능과 연관된 정보의 제 2 부분을 획득하기 위한 수단, 및 정보의 획득된 제 2 부분에 대한 액세스를 가능하게 하기 위해 정보의 리트리브된 제 1 부분을 사용하여 기능에 대한 액세스를 가능하게 하기 위한 수단을 제공할 수 있다. 한 양상에서, SE(560)는 프로세서(506), RAM 및 NVM을 포함할 수 있다. 한 양상에서, 보안 컴포넌트(562)는 프로세서 및 RAM을 포함할 수 있다. 한 양상에서, 비보안 컴포넌트(564)는 NVM의 실질적인 전부를 포함할 수 있다.

[0037] 본 명세서에서 설명된 데이터 저장소(예를 들어, 메모리(508))는 휘발성 메모리 또는 NVM일 수 있고, 또는 휘발성 메모리와 NVM를 모두 포함할 수 있다고 인식될 것이다. 한정이 아닌 예시로, 비휘발성 메모리는 판독 전용

메모리(ROM), 프로그래밍 가능 ROM(PROM: programmable ROM), 전기적으로 프로그래밍 가능한 ROM(EPROM: electrically programmable ROM), 전기적으로 소거 가능한 PROM(EEPROM) 또는 플래시 메모리를 포함할 수 있다. 휘발성 메모리는 외부 캐시 메모리 역할을 하는 랜덤 액세스 메모리(RAM)를 포함할 수 있다. 한정이 아닌 예시로, RAM은 동기식 RAM(SRAM: synchronous RAM), 동적 RAM(DRAM: dynamic RAM), 동기식 DRAM(SDRAM: synchronous DRAM), 2배속 SDRAM(DDR SDRAM: double data rate SDRAM), 확장 SDRAM(ESDRAM: enhanced SDRAM), 싱크링크 DRAM(SLDRAM: Synchlink DRAM) 및 다이렉트 램버스 RAM(DRRAM: direct Rambus RAM)과 같은 많은 형태들로 이용 가능하다. 본 발명의 시스템들 및 방법들의 메모리(508)는 이러한 그리고 임의의 다른 적당한 타입들의 메모리를, 이들로 한정하지 않으면서 포함할 수 있다.

[0038] 다른 양상에서, 통신 디바이스(500)는 NFC 제어기 인터페이스(NCI: NFC controller interface)(550)를 포함할 수 있다. 한 양상에서, NCI(550)는 NFC 가능 안테나(예를 들어, 502, 520)와 NFC 제어기(530) 간의 통신들을 가능하게 하도록 동작 가능할 수 있다. NCI(550)는 청취 모드 및/또는 폴링 모드로 기능하도록 구성 가능할 수도 있다.

[0039] 다른 양상에서, 통신 디바이스(500)는 하나 또는 그보다 많은 보안 엘리먼트들(560)을 포함할 수 있다. 한 양상에서, 하나 또는 그보다 많은 보안 엘리먼트들(560)은 NFC 제어기(530)에 커플링될 수 있고 그리고/또는 NFC 제어기(530) 내에 적어도 부분적으로 통합될 수 있다. 한 양상에서, 하나 또는 그보다 많은 보안 엘리먼트들(560)은 MSM 칩(예를 들어, 프로세서(506))에 커플링될 수 있고 그리고/또는 MSM 칩(예를 들어, 프로세서(506))에 적어도 부분적으로 통합될 수 있다. 한 양상에서, 하나 또는 그보다 많은 보안 엘리먼트들(560)은 보안 엘리먼트들 또는 근접장 제어기 실행 환경(NFCEE: near field controller execution environment)들일 수 있다. 한 양상에서, 하나 또는 그보다 많은 보안 엘리먼트들(560)은 SIM, CSIM 등과 같은, 그러나 이에 한정된 것은 아닌 다양한 모듈들을 가진 UICC를 포함할 수 있다. 다른 양상에서, 하나 또는 그보다 많은 보안 엘리먼트들(560)은 도 4에서 설명된 프로세스들을 수행하도록 구성될 수 있다.

[0040] SE(560)는 보안 컴포넌트(562) 및 비보안 컴포넌트(564)를 포함할 수 있다. 보안 컴포넌트(562)와 비보안 컴포넌트(564)는 인터페이스를 통해 커플링될 수 있다. 한 양상에서, 인터페이스는 암호화를 지원하는 버스 인터페이스를 사용하도록 구성될 수 있다. 다른 양상에서, 인터페이스는 표준 고속 인터페이스일 수 있다. 이러한 양상에서, 인터페이스는 처리를 위해 비보안 메모리(570)로부터 SE(560)의 보안 컴포넌트(562)로의 코드, 애플릿들 등의 효율적인 로딩을 제공한다.

[0041] 보안 컴포넌트(562)는 보안 메모리(568)를 포함할 수 있다. 한 양상에서, 보안 메모리(568)는 보호(예를 들어, 루트 키들, 인증서들 등)로부터 이익을 얻을 수 있는 다양한 아이템들을 저장하기에 충분한 메모리를 포함할 수 있다. 한 양상에서, 보안 메모리(568)는 5 내지 10kbits의 공간을 포함할 수 있다. 한 양상에서, 보안 메모리(568)는 비보안 메모리(570)에 저장된 정보의 효율적인 로딩 및 처리를 가능하게 하기에 충분한 저장 능력을 포함할 수 있다.

[0042] 또한, 보안 컴포넌트(562)는 보안성 차폐(566)를 사용하여 보안이 확보될 수 있다. 한 양상에서, 보안성 차폐(566)는 하드웨어 기반 공격들에 대한 다양한 예방책들, 예컨대 내부 동작의 관찰을 더 어렵게 하는 금속층들, 패키지가 열리면 동작을 불가능하게 하는 광 센서들, 유사한 동작들에 대한 다수의 하드웨어 경로들 등(그러나 이들에 한정된 것은 아님)을 제공할 수 있다. 한 양상에서, 보안성 차폐(566)는 SoC와 연관된 기존 금속층들을 사용하여 보안성 차폐 형태들에 대한 디지털 또는 아날로그 IP를 구현할 수 있다.

[0043] 비보안 컴포넌트(564)는 비보안 메모리(570)를 포함할 수 있다. 한 양상에서, 비보안 메모리(570)는 보안 저장소, 표준 NVM, 또는 이들의 임의의 결합을 제공하는 작업으로 특수화될 수 있다. 한 양상에서, 비보안 메모리(570)는 대략 1.2Mbytes의 공간으로 구성될 수 있다. 다른 양상에서, 비보안 메모리(570)는 SE(560)를 통해 액세스 가능한 다양한 기능들과 연관된 코드, 애플릿들 등을 저장하는데 사용될 수도 있다. 이러한 양상에서, 비보안 메모리(570)는 애플리케이션들(예를 들어, 컴퓨터 코드) 및 데이터의 비휘발성 저장소에 사용될 수 있고, 보안 메모리(568)는 애플리케이션들과 연관된 키 시스템을 저장하는데 사용될 수 있다. 한 양상에서는, 외부 인터페이스를 통한 공격들에 대해 코드 및 데이터의 보안성 및 무결성을 유지하는데 도움이 되도록, 데이터가 SE(560)를 떠날 때마다 데이터가 (보안을 확보하도록) 암호화되고 (무결성을 보장하도록) 서명될 수 있다. 이에 따라, 비보안 메모리(570) 내의 정보는 보안 컴포넌트(562) 내에서 사용되는 암호화 연산들에 의해 제공되는 능력 범위까지 보안이 확보될 수 있다.

[0044] 추가로, 통신 디바이스(500)는 사용자 인터페이스(540)를 포함할 수 있다. 사용자 인터페이스(540)는 통신 디바이스(500)로의 입력들을 생성하기 위한 입력 메커니즘들(542) 및 통신 디바이스(500)의 사용자에 의한 소비를

위한 정보를 생성하기 위한 출력 메커니즘(544)을 포함할 수 있다. 예를 들어, 입력 메커니즘들(542)은 키 또는 키보드, 마우스, 터치스크린 디스플레이, 마이크로폰 등과 같은 메커니즘을 포함할 수 있다. 또한, 예를 들어 출력 메커니즘(544)은 디스플레이, 오디오 스피커, 햅틱 피드백 메커니즘, 개인 영역 네트워크(PAN: Personal Area Network) 트랜시버 등을 포함할 수 있다. 예시된 양상들에서, 출력 메커니즘(544)은 이미지 또는 비디오 포맷인 미디어 콘텐츠를 제시하도록 동작 가능한 디스플레이 또는 오디오 포맷인 미디어 콘텐츠를 제시하기 위한 오디오 스피커를 포함할 수 있다.

[0045] 도 6은 통신 디바이스에 적어도 부분적으로 통합될 수 있는 SE(308)로 효율적인 기능을 가능하게 하도록 동작 가능한 예시적인 통신 시스템(600)의 블록도를 도시한다. 예를 들어, 통신 시스템(600)은 통신 디바이스(예를 들어, 통신 디바이스(500)) 내에 적어도 부분적으로 상주할 수 있다. 또한, SE(308)는 통신 디바이스(예를 들어, 통신 디바이스(500)) 내에 적어도 부분적으로 상주할 수 있다. 시스템(600)은 프로세서, 소프트웨어, 또는 이들의 결합(예를 들어, 펌웨어)에 의해 구현되는 기능들을 나타내는 기능 블록들일 수 있는 기능 블록들을 포함하는 것으로 표현된다고 인식되어야 한다. 시스템(600)은 결합하여 작동할 수 있는 전기 컴포넌트들의 로직 그룹(602)을 포함한다.

[0046] 예컨대, 로직 그룹(602)은 SE에 저장된 정보를 통해 액세스 가능한 기능에 액세스하기 위한 요청을 수신하기 위한 수단(604)을 제공할 수 있는 전기 컴포넌트를 포함할 수 있다. 예를 들어, 수신하기 위한 수단(604)은 SE(308)의 보안 컴포넌트(310) 및 프로세서(312), 그리고/또는 통신 디바이스(500)의 프로세서(506)를 포함할 수 있다.

[0047] 또한, 로직 그룹(602)은 SE의 보안 컴포넌트에 저장된, 기능과 연관된 정보의 제 1 부분을 리트리브하기 위한 수단(606)을 제공할 수 있는 전기 컴포넌트를 포함할 수 있다. 한 양상에서, 보안 컴포넌트는 프로세서 및 RAM을 포함할 수 있다. 예를 들어, 리트리브하기 위한 수단(606)은 SE(308)의 보안 컴포넌트(310), 보안 NVM(314) 및/또는 프로세서(312)를 포함할 수 있다.

[0048] 또한, 로직 그룹(602)은 SE의 비보안 컴포넌트에 저장된, 기능과 연관된 정보의 제 2 부분을 획득하기 위한 수단(608)을 제공할 수 있는 전기 컴포넌트를 포함할 수 있다. 한 양상에서, 비보안 컴포넌트는 NVM의 실질적인 전부를 포함할 수 있다. 예를 들어, 획득하기 위한 수단(608)은 SE(308)의 보안 컴포넌트(310), 비보안 컴포넌트(320), 보안 NVM(314), 비보안 메모리(322) 및/또는 프로세서(312)를 포함할 수 있다. 한 양상에서, 획득하기 위한 수단(608)은 SE의 비보안 컴포넌트와 SE의 보안 컴포넌트 사이의 고속 인터페이스를 사용하도록 구성될 수 있다.

[0049] 더욱이, 로직 그룹(602)은 정보의 획득된 제 2 부분에 대한 액세스를 가능하게 하기 위해 정보의 리트리브된 제 1 부분을 사용하여 기능에 대한 액세스를 가능하게 하기 위한 수단(610)을 제공할 수 있는 전기 컴포넌트를 포함할 수 있다. 한 양상에서, 액세스를 가능하게 하기 위한 수단(610)은 SE(308)의 보안 컴포넌트(310), 비보안 컴포넌트(320), 보안 NVM(314), 비보안 메모리(322) 및/또는 프로세서(312)를 포함할 수 있다.

[0050] 선택적인 양상에서, 로직 그룹(602)은 기능과 연관된 정보를 복호화하기 위한 수단(612)을 제공할 수 있는 전기 컴포넌트를 포함할 수 있다. 예를 들어, 복호화하기 위한 수단(612)은 SE(308)의 보안 컴포넌트(310) 및/또는 프로세서(312)를 포함할 수 있다.

[0051] 추가로, 시스템(600)은 전기 컴포넌트들(604, 606, 608, 610, 612)과 연관된 기능들을 실행하기 위한 명령들을 보유하며, 전기 컴포넌트들(604, 606, 608, 610, 612)에 의해 사용되거나 획득되는 데이터를 저장하는 등의 메모리(614)를 포함할 수 있다. 한 양상에서, 메모리(614)는 메모리(508)를 포함할 수 있고 그리고/또는 메모리(508)에 포함될 수 있다. 메모리(614) 외부에 있는 것으로 도시되었지만, 전기 컴포넌트들(604, 606, 608, 610, 612) 중 하나 또는 그보다 많은 전기 컴포넌트는 메모리(614) 내부에 존재할 수 있다고 이해되어야 한다. 일례로, 전기 컴포넌트들(604, 606, 608, 610, 612)이 적어도 하나의 프로세서를 포함할 수 있고, 또는 각각의 전기 컴포넌트(604, 606, 608, 610, 612)가 적어도 하나의 프로세서의 해당 모듈일 수 있다. 더욱이, 추가적인 또는 대안적인 예에서, 전기 컴포넌트들(604, 606, 608, 610, 612)은 컴퓨터 판독 가능 매체를 포함하는 컴퓨터 프로그램 물건일 수 있으며, 여기서 각각의 전기 컴포넌트(604, 606, 608, 610, 612)는 대응하는 코드일 수 있다.

[0052] 본 출원에서 사용된 바와 같이, "컴포넌트," "모듈," "시스템" 등의 용어들은 하드웨어, 펌웨어, 하드웨어와 소프트웨어의 결합, 소프트웨어, 또는 실행중인 소프트웨어와 같은, 그러나 이에 한정된 것은 아닌 컴퓨터 관련 엔티티를 포함하는 것으로 의도된다. 예를 들어, 컴포넌트는 프로세서 상에서 실행하는 프로세스, 프로세서,

객체, 실행 파일(executable), 실행 스레드, 프로그램 및/또는 컴퓨터일 수도 있지만, 이에 한정된 것은 아니다. 예시로, 컴퓨팅 디바이스 상에서 실행하는 애플리케이션과 컴퓨팅 디바이스 모두 컴포넌트일 수 있다. 하나 또는 그보다 많은 컴포넌트들이 프로세스 및/또는 실행 스레드 내에 상주할 수 있으며, 컴포넌트가 하나의 컴퓨터에 집중될 수도 있고 그리고/또는 2개 또는 그보다 많은 컴퓨터들 사이에 분산될 수도 있다. 또한, 이러한 컴포넌트들은 다양한 데이터 구조들이 저장된 다양한 컴퓨터 판독 가능 매체들로부터 실행될 수 있다. 컴포넌트들은 예컨대, 하나 또는 그보다 많은 데이터 패킷들(예를 들면, 로컬 시스템에서, 분산 시스템에서, 그리고/또는 신호에 의해 다른 시스템들과의 네트워크(예를 들어, 인터넷)를 통해 다른 컴포넌트와 상호 작용하는 하나의 컴포넌트로부터의 데이터)을 갖는 신호에 따라 로컬 및/또는 원격 프로세스들을 통해 통신할 수 있다.

[0053] 더욱이, 본 명세서에서는 유선 단말 또는 무선 단말일 수 있는 단말과 관련하여 다양한 양상들이 설명된다. 단말은 또한 시스템, 디바이스, 가입자 유닛, 가입자국, 이동국, 모바일, 모바일 디바이스, 원격국, 모바일 장비(ME: mobile equipment), 원격 단말, 액세스 단말, 사용자 단말, 단말, 통신 디바이스, 사용자 에이전트, 사용자 디바이스 또는 사용자 장비(UE: user equipment)로 지칭될 수도 있다. 무선 단말은 셀룰러 전화, 위성 전화, 코드리스 전화, 세션 개시 프로토콜(SIP: Session Initiation Protocol) 전화, 무선 로컬 루프(WLL: wireless local loop) 스테이션, 개인용 디지털 보조기기(PDA), 무선 접속 능력을 가진 핸드헬드 디바이스, 컴퓨팅 디바이스, 또는 무선 모뎀에 접속된 다른 처리 디바이스들일 수 있다. 더욱이, 본 명세서에서는 기지국과 관련하여 다양한 양상들이 설명된다. 기지국은 무선 단말(들)과의 통신에 이용될 수 있으며, 또한 액세스 포인트, 노드 B, 또는 다른 어떤 용어로 지칭될 수도 있다.

[0054] 더욱이, "또는"이라는 용어는 배타적 "또는"보다는 포괄적 "또는"을 의미하는 것으로 의도된다. 즉, 달리 명시되지 않거나 맥락상 명확하지 않다면, "X는 A 또는 B를 이용한다"라는 문구는 당연히 포괄적 치환들 중 임의의 치환을 의미하는 것으로 의도된다. 즉, "X는 A 또는 B를 이용한다"라는 문구는 X가 A를 이용하는 경우; X가 B를 이용하는 경우; 또는 X가 A와 B를 모두 이용하는 경우 중 임의의 경우에 의해 충족된다. 또한, 본 출원 및 첨부된 청구항들에서 사용되는 단수 표현들은 달리 명시되지 않거나 맥락상 단수 형태로 지시되는 것으로 명확하지 않다면, 일반적으로 "하나 또는 그보다 많은 것"을 의미하는 것으로 해석되어야 한다.

[0055] 본 명세서에서 설명되는 기술들은 CDMA, TDMA, FDMA, OFDMA, SC-FDMA 및 다른 시스템들과 같은 다양한 무선 통신 시스템들에 사용될 수 있다. "시스템"과 "네트워크"라는 용어들은 흔히 상호 교환 가능하게 사용된다. CDMA 시스템은 범용 지상 무선 액세스(UTRA: Universal Terrestrial Radio Access), cdma2000 등과 같은 무선 기술을 구현할 수 있다. UTRA는 광대역 CDMA(W-CDMA) 및 CDMA의 다른 변형들을 포함한다. 또한, cdma2000은 IS-2000, IS-95 및 IS-856 표준들을 커버한다. TDMA 시스템은 글로벌 모바일 통신 시스템(GSM: Global System for Mobile Communications)과 같은 무선 기술을 구현할 수 있다. OFDMA 시스템은 진화형 UTRA(E-UTRA: Evolved UTRA), 울트라 모바일 브로드밴드(UMB: Ultra Mobile Broadband), IEEE 802.11(Wi-Fi), IEEE 802.16(WiMAX), IEEE 802.20, 플래시-OFDMA 등과 같은 무선 기술을 구현할 수 있다. UTRA 및 E-UTRA는 범용 모바일 통신 시스템(UMTS: Universal Mobile Telecommunication System)의 일부이다. 3GPP 롱 텀 에볼루션(LTE: Long Term Evolution)은 다운링크에 대해서는 OFDMA를 그리고 업링크에 대해서는 SC-FDMA를 이용하는 E-UTRA를 사용하는 UMTS의 릴리스이다. UTRA, E-UTRA, UMTS, LTE 및 GSM은 "3세대 파트너십 프로젝트"(3GPP: 3rd Generation Partnership Project)로 명명된 조직으로부터의 문서들에 기술되어 있다. 추가로, cdma2000 및 UMB는 "3세대 파트너십 프로젝트 2"(3GPP2)로 명명된 조직으로부터의 문서들에 기술되어 있다. 또한, 이러한 무선 통신 시스템들은 흔히 언페어드(unpaired) 비허가 스펙트럼들, 802.xx 무선 LAN, 블루투스, 근접장 통신들(NFC-A, NFC-B, NFC-F 등) 그리고 임의의 다른 단거리 또는 장거리 무선 통신 기술들을 이용하는 피어-투-피어(예를 들어, 모바일-투-모바일) 애드 혹 네트워크 시스템들을 추가로 포함할 수 있다.

[0056] 다수의 디바이스들, 컴포넌트들, 모듈들 등을 포함할 수 있는 시스템들에 관하여 다양한 양상들 또는 특징들이 제시될 것이다. 다양한 시스템들은 추가 디바이스들, 컴포넌트들, 모듈들 등을 포함할 수도 있고 그리고/또는 도면들과 관련하여 논의되는 디바이스들, 컴포넌트들, 모듈들 등의 전부를 포함하는 것은 아닐 수도 있다고 이해 및 인식되어야 한다. 이러한 접근 방식들의 결합이 또한 사용될 수도 있다.

[0057] 본 명세서에 개시된 양상들과 관련하여 설명된 다양한 예시적인 로직들, 로직 블록들, 모듈들 및 회로들은 범용 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 가능 로직 디바이스, 이산 게이트 또는 트랜지스터 로직, 이산 하드웨어 컴포넌트들, 또는 본 명세서에서 설명된 기능들을 수행하도록 설계된 이들의 임의의 결합으로 구현 또는 수행될 수 있다. 범용 프로세서는 마이크로프로세서일 수도 있지만, 대안으로 프로세서는 임의의 종래 프로세서, 제어기, 마이크로

컨트롤러 또는 상태 머신일 수도 있다. 프로세서는 또한 컴퓨팅 디바이스들의 결합, 예를 들어 DSP와 마이크로프로세서의 결합, 복수의 마이크로프로세서들, DSP 코어와 결합한 하나 또는 그보다 많은 마이크로프로세서들, 또는 임의의 다른 이러한 구성으로서 구현될 수도 있다. 추가로, 적어도 하나의 프로세서는 위에서 설명한 단계들 및/또는 동작들 중 하나 또는 그보다 많은 것을 수행하도록 동작 가능한 하나 또는 그보다 많은 모듈들을 포함할 수 있다.

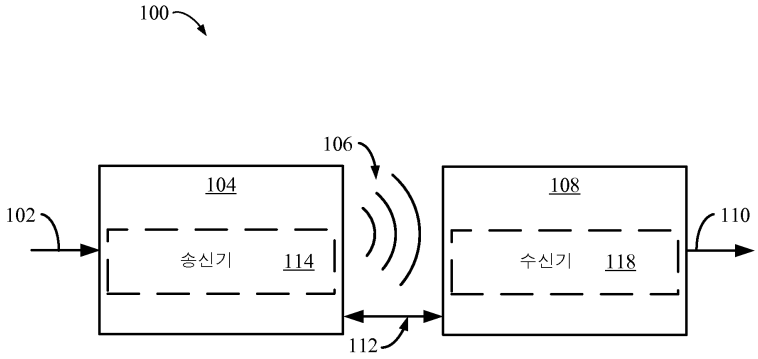
[0058] 또한, 본 명세서에 개시된 양상들과 관련하여 설명된 방법 또는 알고리즘의 단계들 및/또는 동작들은 직접 하드웨어로, 프로세서에 의해 실행되는 소프트웨어 모듈로, 또는 이 둘의 조합으로 구현될 수 있다. 소프트웨어 모듈은 RAM 메모리, 플래시 메모리, ROM 메모리, EPROM 메모리, EEPROM 메모리, 레지스터들, 하드디스크, 착탈식 디스크, CD-ROM, 또는 해당 기술분야에 공지된 임의의 다른 형태의 저장 매체에 상주할 수 있다. 예시적인 저장 매체는 프로세서가 저장 매체로부터 정보를 읽고 저장 매체에 정보를 기록할 수 있도록 프로세서에 연결될 수 있다. 대안으로, 저장 매체는 프로세서에 통합될 수도 있다. 또한, 일부 양상들에서 프로세서 및 저장 매체는 ASIC에 상주할 수도 있다. 추가로, ASIC는 사용자 단말에 상주할 수도 있다. 대안으로, 프로세서 및 저장 매체는 사용자 단말에 개별 컴포넌트들로서 상주할 수도 있다. 추가로, 일부 양상들에서, 방법 또는 알고리즘의 단계들 및/또는 동작들은 컴퓨터 프로그램 물건으로 통합될 수 있는 컴퓨터 판독 가능 매체 및/또는 기계 판독 가능 매체 상에 코드들 및/또는 명령들 중 하나 또는 이들의 임의의 조합 또는 세트로서 상주할 수 있다.

[0059] 하나 또는 그보다 많은 양상들에서, 설명된 기능들은 하드웨어, 소프트웨어, 펌웨어, 또는 이들의 임의의 결합으로 구현될 수 있다. 소프트웨어로 구현된다면, 이 기능들은 컴퓨터 판독 가능 매체 상에 하나 또는 그보다 많은 명령들 또는 코드로서 저장되거나 전송될 수 있다. 컴퓨터 판독 가능 매체는 한 장소에서 다른 장소로 컴퓨터 프로그램의 전달을 용이하게 하는 임의의 매체를 포함하는 통신 매체와 컴퓨터 저장 매체를 모두 포함한다. 저장 매체는 컴퓨터에 의해 액세스 가능한 임의의 이용 가능한 매체일 수 있다. 한정이 아닌 예시로, 이러한 컴퓨터 판독 가능 매체는 RAM, ROM, EEPROM, CD-ROM이나 다른 광 디스크 저장소, 자기 디스크 저장소 또는 다른 자기 저장 디바이스들, 또는 명령들이나 데이터 구조들의 형태로 원하는 프로그램 코드를 전달 또는 저장하는데 사용될 수 있으며 컴퓨터에 의해 액세스 가능한 임의의 다른 매체를 포함할 수 있다. 또한, 임의의 접속이 컴퓨터 판독 가능 매체로 지칭될 수 있다. 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 보통 데이터를 레이저들에 의해 광학적으로 재생한다. 상기의 결합들 또한 컴퓨터 판독 가능 매체의 범위 내에 포함되어야 한다.

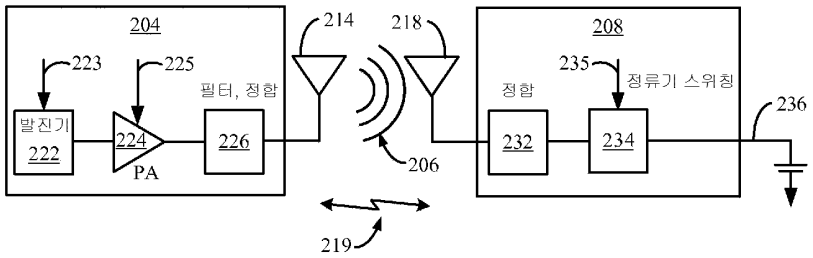
[0060] 앞서 말한 개시는 예시적인 양상들 및/또는 실시예들을 논의하지만, 첨부된 청구항들에 의해 정의된 바와 같은, 설명된 양상들 및/또는 실시예들의 범위를 벗어나지 않으면서 본 명세서에 다양한 변경들 및 수정들이 이루어질 수 있다는 점에 유의해야 한다. 더욱이, 설명된 양상들 및/또는 실시예들의 엘리먼트들은 단수로 설명 또는 청구될 수 있지만, 단수로의 한정이 명시적으로 언급되지 않는 한 다수가 고려된다. 추가로, 달리 언급되지 않는 한, 임의의 양상 및/또는 실시예의 일부 또는 전부가 임의의 다른 양상 및/또는 실시예의 일부 또는 전부와 함께 이용될 수도 있다.

도면

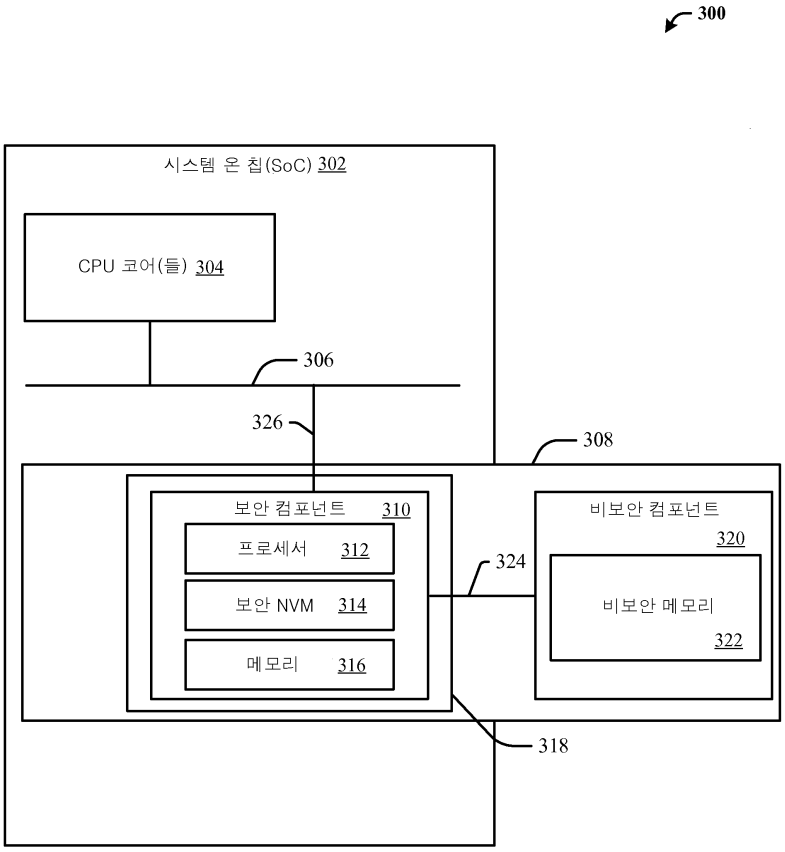
도면1


100
106
104
108
102
110
송신기
114
수신기
118
112

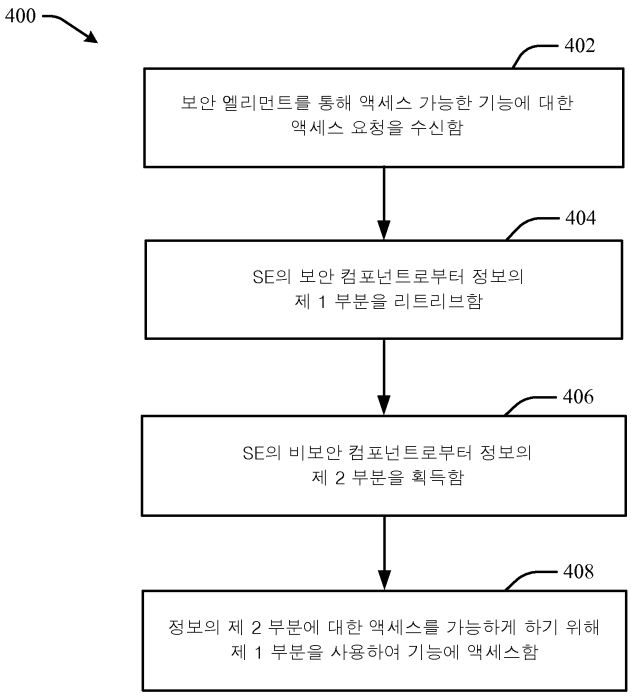
도면2


204
214
218
208
223
225
235
정류기 스위칭
필터, 정합
정합
발진기
222
224
PA
226
232
234
236
206
219

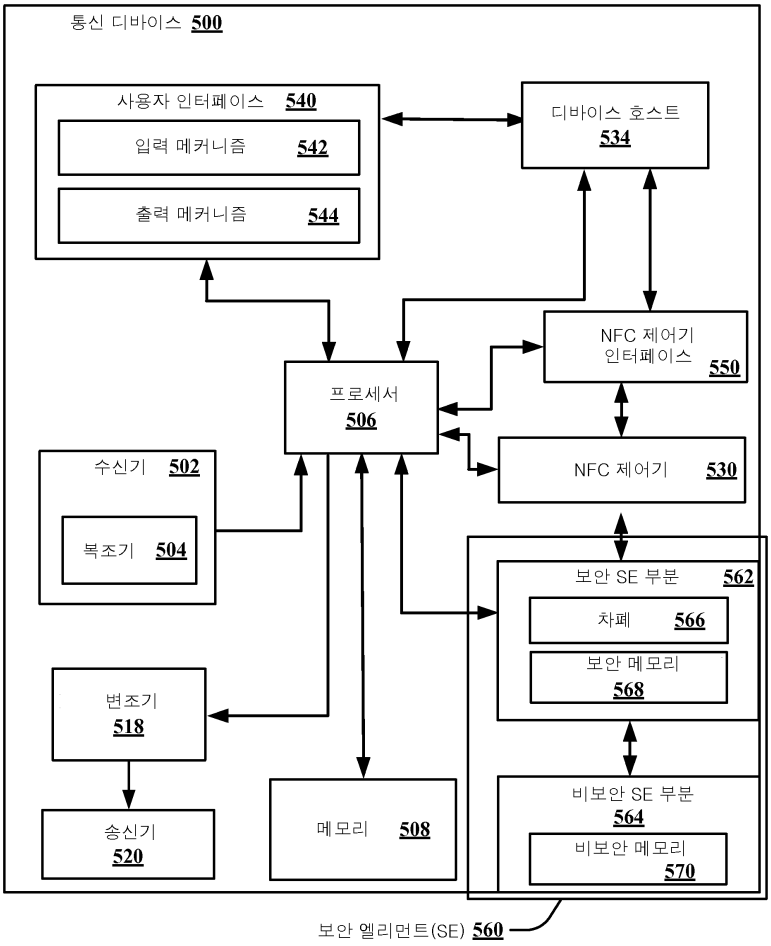
도면3


300
시스템 온 칩(SoC) 302
CPU 코어(들) 304
306
326
308
보안 컴포넌트 310
프로세서 312
보안 NVM 314
메모리 316
324
비보안 컴포넌트
320
비보안 메모리
322
318

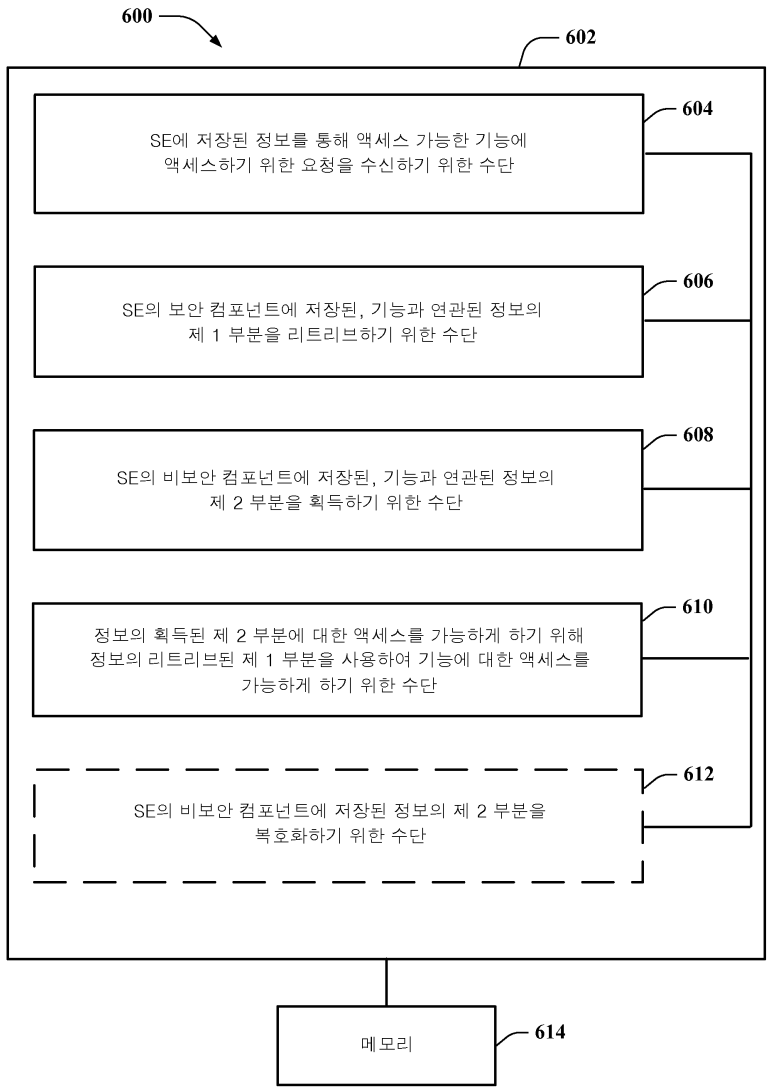
도면4


400
402
보안 엘리먼트를 통해 액세스 가능한 기능에 대한 액세스 요청을 수신함
404
SE의 보안 컴포넌트로부터 정보의 제 1 부분을 리트리브함
406
SE의 비보안 컴포넌트로부터 정보의 제 2 부분을 획득함
408
정보의 제 2 부분에 대한 액세스를 가능하게 하기 위해 제 1 부분을 사용하여 기능에 액세스함

도면5


통신 디바이스 500
사용자 인터페이스 540
입력 메커니즘 542
출력 메커니즘 544
디바이스 호스트 534
NFC 제어기 인터페이스 550
프로세서 506
NFC 제어기 530
수신기 502
복조기 504
보안 SE 부분 562
차폐 566
보안 메모리 568
변조기 518
비보안 SE 부분 564
비보안 메모리 570
송신기 520
메모리 508
보안 엘리먼트(SE) 560

도면6


600
602
SE에 저장된 정보를 통해 액세스 가능한 기능에 액세스하기 위한 요청을 수신하기 위한 수단
604
SE의 보안 컴포넌트에 저장된, 기능과 연관된 정보의 제 1 부분을 리트리브하기 위한 수단
606
SE의 비보안 컴포넌트에 저장된, 기능과 연관된 정보의 제 2 부분을 획득하기 위한 수단
608
정보의 획득된 제 2 부분에 대한 액세스를 가능하게 하기 위해 정보의 리트리브된 제 1 부분을 사용하여 기능에 대한 액세스를 가능하게 하기 위한 수단
610
SE의 비보안 컴포넌트에 저장된 정보의 제 2 부분을 복호화하기 위한 수단
612
메모리
614