(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2009-0065415
(43) 공개일자 2009년06월22일

(51) Int. Cl.
G06F 21/00 (2006.01)
(21) 출원번호 10-2008-0064922
(22) 출원일자 2008년07월04일
심사청구일자 2008년07월04일
(30) 우선권주장
1020070132627 2007년12월17일 대한민국(KR)

(71) 출원인
한국전자통신연구원
대전 유성구 가정동 161번지
(72) 발명자
박영수
대전 서구 탄방동 산호아파트 101동 907호
박지만
대전 유성구 송강동 청솔아파트 310동 1208호
(뒷면에 계속)
(74) 대리인
유미특허법인

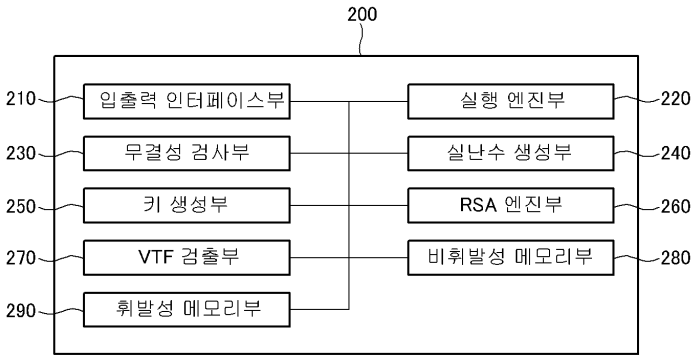
전체 청구항 수 : 총 13 항

(54) 플랫폼 장착용 모듈 및 플랫폼 장착용 모듈을 위한 기능변경 방법

(57) 요 약

플랫폼 장착용 모듈은 입출력 인터페이스부를 통해 외부 장치와 통신할 수 있고, 내장된 펌웨어 및 입출력 인터페이스부로 수신된 명령을 실행하여 데이터 처리 내부 제어 신호 발생 등의 제어를 수행하는 실행 엔진부, 해시 연산을 통해 인증 절차를 수행하여 무결성을 검사하는 무결성 검사부, 대칭키 쌍 및 RSA 암호키 쌍을 생성하는 키 생성부, RSA 암호 연산을 이용하여 데이터를 암호화하여 암호화된 데이터를 생성하는 RSA 엔진부, RSA 암호키 쌍 및 암호화된 데이터를 저장하고, 플랫폼 장착용 모듈과 연관된 식별자 및 상태를 저장하는 비휘발성 메모리부, 동적 데이터를 저장하는 휘발성 메모리부, 난수를 생성하는 실난수 생성부 및 입출력 인터페이스부를 통한 외부의 오류 주입 공격에 대비하여 동작 규격 이외의 전압, 온도 및 동작 주파수의 값에 대한 검출과 플랫폼 장착용 모듈의 실행을 차단하는 제어 신호를 생성하는 VTF 검출부를 포함한다. 이를 통해 모바일 디바이스의 키의 생성과 무결성을 보장하고, 미리 설정된 플랫폼 장착용 모듈의 기능을 변경할 수 있다.

대 표 도 - 도2



(72) 발명자

김무섭

대전 유성구 관평동 대덕테크노밸리 6단지 606동 1002호

주홍일

대전 서구 월평3동 311 다모아아파트 105동 1102호

김영세

대전 유성구 상대동 유성목련아파트 101동 1001호

전성익

대전 유성구 어은동 한빛아파트 107동 704호

이 발명을 지원한 국가연구개발사업

과제고유번호	2006-S-041-02
부처명	정보통신부 및 정보통신연구진흥원
연구사업명	IT성장동력기술개발
연구과제명	차세대 모바일 단말기의 보안 및 신뢰 서비스를 위한 공통보안 핵심 모듈 개발
주관기관	한국전자통신연구원
연구기간	2007.03.01~2008.02.28

특허청구의 범위

청구항 1

모바일 디바이스와 통신을 위한 인터페이스를 제공하는 입출력 인터페이스부;

미리 저장된 제1 코드에 대응하는 펌웨어를 실행하여 데이터를 생성하는 실행 엔진부;

해시 연산을 통해 인증 절차를 수행하여 무결성을 보장하는 무결성 검사부;

대칭키 쌍 및 알에스에이 암호화 방식에 대응하는 암호키 쌍을 생성하는 키 생성부;

상기 암호키 쌍을 이용하여 상기 데이터를 암호화하여 암호화된 데이터를 생성하는 암호화 엔진부;

동적 데이터를 저장하는 휘발성 메모리부;

임의의 연속적인 수에 해당하는 난수를 생성하는 실난수 생성부;

상기 입출력 인터페이스부를 통한 물리적 오류를 검출하여 상기 물리적 오류에 대응하는 리셋 신호를 생성하는 물리적 오류 검출부; 및

상기 제1 코드를 저장하고, 상기 입출력 인터페이스부를 통해 모드 선택 신호를 수신하여 상기 모드 선택 신호를 바탕으로 상기 실행 엔진부로 상기 제1 코드 이외의 코드를 제공하는 비휘발성 메모리부를 포함하는 플랫폼 장착용 모듈.

청구항 2

제1항에 있어서,

상기 비휘발성 메모리부는

상기 입출력 인터페이스부를 통해 상기 모바일 디바이스에 해당하는 외부 메모리와 통신하고, 상기 실행 엔진부와 통신하는 외부 메모리 제어부;

전원이 공급되지 않아도 저장된 정보를 계속 유지하며, 상기 제1 코드, 상기 암호화된 데이터, 상기 대칭키 쌍 및 상기 암호키 쌍을 저장하는 비휘발성 메모리;

상기 비휘발성 메모리를 제어하고, 상기 실행 엔진부와 통신하는 내부 메모리 제어부; 및

상기 모드 선택 신호에 따라 상기 외부 메모리 제어부 및 상기 내부 메모리 제어부를 제어하는 모드 입출력 제어부를 포함하는 플랫폼 장착용 모듈.

청구항 3

제1항에 있어서,

상기 키 생성부는

키 생성 코드에 따라 키 생성 제어 신호를 생성하는 키 생성 제어부;

난수를 바탕으로 상기 키 생성 제어 신호에 따라 소수 쌍을 생성하는 소수 생성부; 및

상기 소수 쌍을 바탕으로 공개 키 및 개인 키를 포함하는 상기 암호키 쌍을 생성하는 암호키 생성부를 포함하는 플랫폼 장착용 모듈.

청구항 4

제1항에 있어서,

상기 입출력 인터페이스부는

일반적인 용도로 사용이 가능한 입출력 모듈에 해당하고, 통상의 입출력 단자를 가지는 범용 입출력 모듈;

모뎀 또는 직렬 통신 장치와 통신하여 데이터를 송수신할 수 있는 모듈에 해당하고, 통상의 입출력 단자를 가지는 범용 비동기 송수신 모듈;

범용 2-핀 직렬 통신 모듈에 해당하고, 통상의 입출력 단자를 가지는 투와이어 인터페이스 모듈; 및

상기 비휘발성 메모리부와 상기 모바일 디바이스간의 인터페이스를 제공하는 로컬 입출력 모듈을 포함하는 플랫폼 장착용 모듈.

청구항 5

제1항에 있어서,

상기 무결성 검사부는

상기 입출력 인터페이스부를 통해 사용자 인증 메시지를 포함하는 사용자 인증 신호를 입력 받는 입력 제어부;

상기 사용자 인증 메시지에 대해 해시 연산을 수행하여 상기 사용자 인증 메시지에 대응하는 해시 연산값을 생성하는 해시 연산부; 및

상기 해시 연산값이 미리 정해진 값에 대응하는 값인지를 검사하고, 검사 결과에 따라 출력을 제어하는 출력 제어부를 포함하는 플랫폼 장착용 모듈.

청구항 6

제1항에 있어서,

상기 암호화 엔진부는

상기 암호화 엔진부의 입력 데이터 및 출력 데이터를 처리하는 데이터 입출력부;

상기 입력 데이터 및 상기 출력 데이터를 임시 저장하는 데이터 임시저장부;

비트 가변적인 처리 구조를 가지고, 알에스에이 암호화 연산을 수행하는 알에스에이 연산부; 및

상기 알에스에이 연산부가 생성하는 중간 데이터 값을 저장하는 중간값 저장부를 포함하는 플랫폼 장착용 모듈.

청구항 7

제1항에 있어서,

상기 실난수 생성부는

난수가 필요한 경우 난수를 생성하기 위한 난수 생성 제어 신호를 생성하는 난수 생성 제어부;

상기 난수 생성 제어 신호에 따라 시드를 생성하는 시드 생성부; 및

상기 시드를 바탕으로 난수를 발생시키는 난수 발생부를 포함하는 플랫폼 장착용 모듈.

청구항 8

제1항에 있어서,

상기 물리적 오류 검출부는

상기 플랫폼 장착용 모듈의 내부의 온도를 감시하여 상기 온도가 미리 정해진 허용 온도 범위를 벗어나면, 상기 온도에 대응하는 온도 제어 신호를 생성하는 온도 감시부;

상기 플랫폼 장착용 모듈에 입력되는 신호의 전압을 감시하여 상기 전압이 미리 정해진 허용 전압 범위를 벗어나면, 상기 전압에 대응하는 전압 제어 신호를 생성하는 전압 감시부;

상기 신호의 주파수를 감시하여 상기 주파수가 미리 정해진 허용 주파수 범위를 벗어나면, 상기 주파수에 대응하는 주파수 제어 신호를 생성하는 주파수 감시부; 및

상기 온도 제어 신호, 상기 전압 제어 신호 또는 상기 주파수 제어 신호를 바탕으로 상기 플랫폼 장착용 모듈의 내부에서 실행 중인 동작을 중지시키고, 동작 중에 생성된 결과를 초기화 시키는 리셋 신호를 생성하는 제어 신호 생성부를 포함하는 플랫폼 장착용 모듈.

청구항 9

제8항에 있어서,

상기 제어 신호 생성부는

상기 플랫폼 장착용 모듈의 클럭 및 전원을 차단시키는 리셋 신호를 생성하는 플랫폼 장착용 모듈.

청구항 10

입출력 인터페이스부, 제1 코드를 저장하는 내부 메모리 및 상기 제1 코드에 대응하는 펌웨어를 실행하는 실행 엔진을 포함하는 플랫폼 장착용 모듈을 위한 기능 변경 방법에 있어서,

상기 플랫폼 장착용 모듈은 상기 입출력 인터페이스부를 통해 제2 코드가 저장된 외부 메모리 또는 제3 코드가 저장된 모바일 장치와 통신하며,

상기 기능 변경 방법은

상기 입출력 인터페이스부를 통해 모드 선택 정보 및 메모리 선택 정보를 포함하는 모드 선택 신호를 수신하는 단계;

상기 모드 선택 정보에 따라 갱신 모드를 실행하는 경우, 상기 모바일 장치로부터 상기 제3 코드를 수신하는 단계; 및

상기 메모리 선택 정보에 따라 상기 내부 메모리에 저장된 코드를 갱신하는 경우, 상기 내부 메모리에 저장된 상기 제1 코드를 상기 제3 코드로 갱신하는 단계를 포함하는 기능 변경 방법.

청구항 11

제10항에 있어서,

상기 기능 변경 방법은

상기 메모리 선택 정보에 따라 상기 외부 메모리에 저장된 코드를 갱신하는 경우, 상기 입출력 인터페이스부를 이용하여 상기 외부 메모리에 저장된 상기 제2 코드를 상기 제3 코드로 갱신하는 단계를 더 포함하는 기능 변경 방법.

청구항 12

제10항에 있어서,

상기 기능 변경 방법은

상기 모드 선택 정보 및 상기 메모리 선택 정보에 따라 상기 외부 메모리에 저장된 코드를 실행하는 경우, 상기 외부 메모리에 저장된 상기 제2 코드를 상기 실행 엔진으로 전달하여 상기 실행 엔진이 상기 제2 코드를 실행하도록 하는 단계를 더 포함하는 기능 변경 방법.

청구항 13

제10항에 있어서,

상기 기능 변경 방법은

상기 모드 선택 정보 및 상기 메모리 선택 정보에 따라 상기 내부 메모리에 저장된 코드를 실행하는 경우, 상기 제3 코드를 수신하는 단계 이전에 상기 내부 메모리에 저장된 상기 제1 코드를 상기 실행 엔진으로 전달하여 상기 실행 엔진이 상기 제1 코드를 실행하도록 하는 단계를 더 포함하는 기능 변경 방법.

명 세 서

발명의 상세한 설명

기 술 분 야

<1> 본 발명은 플랫폼 장착용 모듈 및 플랫폼 장착용 모듈을 위한 기능 변경 방법에 관한 것이다. 특히 본 발명은 모바일용 플랫폼 장착용 모듈 및 모바일용 플랫폼 장착용 모듈을 위한 기능 변경 방법에 관한 것이다.

<2> 본 발명은 정보통신부 및 정보통신연구진흥원의 IT성장동력기술개발사업의 일환으로 수행한 연구로부터 도출된 것이다[과제관리번호: 2006-S-041-02, 과제명: 차세대 모바일 단말기의 보안 및 신뢰 서비스를 위한 공통 보안 핵심 모듈 개발].

배 경 기 술

<3> 휴대폰(Cell Phone), 개인 휴대 정보 단말기(Personal Digital Assistant, PDA) 등과 같은 소형의 모바일 디바이스는 분실 또는 도난되기 쉽기 때문에 악의적인 사용자나 어플리케이션의 표적이 되기 쉽다. 따라서 이러한 모바일 디바이스의 어플리케이션 및 모바일 디바이스에 저장된 데이터를 보호하기 위해 모바일 디바이스의 무결성 보장이 필요하다.

<4> 모바일 디바이스의 무결성 보장은 신뢰성이 보장된 정보 또는 방법을 통해 검증되거나 인정되어야 한다. 이때 모바일 디바이스의 무결성은 하드웨어 컴포넌트를 기반으로 하는 신뢰 플랫폼 모듈(Trusted Platform Module, TPM)을 통해 보장될 수 있다. 또한 시스템-온-칩 또는 주문형 반도체(Application Specific Integrated Circuits, ASIC)에 해당하는 신뢰 플랫폼 모듈(Trusted Platform Module, TPM)을 장착한 모바일 디바이스를 모바일 신뢰 디바이스라고 한다.

<5> 다음은 도 1을 참고하여 종래의 모바일 신뢰 디바이스에 장착되는 신뢰 플랫폼 모듈에 대해 설명한다.

<6> 도 1은 종래의 신뢰 플랫폼 모듈의 구성을 도시한 도면이다.

<7> 도 1에 도시된 바와 같이, 종래의 신뢰 플랫폼 모듈(100)은 입력/출력 컴포넌트(101), 암호 코프로세서(Cryptographic Coprocessor)(103), 키 생성기(105), 해시 기반 메시지 인증 코드 생성기(keyed-Hash for Message Authentication Code 생성기, 이하에서는 'HMAC 생성기'이라고도 함)(107), 난수 발생기(109), 안전한 해쉬 알고리즘-1 엔진(Secure Hash Algorithm-1 엔진, 이하에서는 'SHA-1 엔진'이라고도 함)(111), 전력 검출기(113), 옵트-인 컴포넌트(Opt-In Component)(115), 실행 엔진(117), 비휘발성 메모리(119), 휘발성 메모리(121) 및 키 저장부(123)를 포함한다.

<8> 입력/출력 컴포넌트(101)는 신뢰 플랫폼 모듈(100)의 내부의 통신 버스를 통해 정보 흐름을 관리한다.

<9> 암호 코프로세서(103)는 신뢰 플랫폼 모듈(100)의 내부에서 암호 동작을 수행한다.

<10> 키 생성기(105)는 대칭 암호키 또는 알에스에이 암호키(Rivest Shamir Adleman 암호키, 이하에서는 'RSA 암호키'라고도 함) 쌍을 생성한다.

<11> HMAC 생성기(107)는 메시지 인증 알고리즘을 수행하여, 무결성 검사를 위한 메시지 인증 코드를 생성한다.

<12> 난수 발생기(109)는 신뢰 플랫폼 모듈(100)의 내부에서 여러 가지 값을 계산하기 위한 연속적인 임의의 수에 해당하는 난수를 발생시킨다.

<13> SHA-1 엔진(111)은 안전한 해쉬 알고리즘-1(Secure Hash Algorithm, 이하에서는 'SHA-1'이라고도 함)을 구현한다.

<14> 전력 검출기(113)는 신뢰 플랫폼 모듈(100)의 전력 상태를 관리한다.

<15> 옵트-인 컴포넌트(115)는 지속적인 휘발성 플래그의 상태를 유지하고 신뢰 플랫폼 모듈(100)이 인에이블(enable) 또는 디스에이블(disable)될 수 있도록 플래그와 연관된 시맨틱(semantic)을 실시한다.

<16> 실행 엔진(117)은 입력/출력 컴포넌트(101)를 통해 수신하는 명령에 대응하는 프로그램 코드를 실행한다.

<17> 비휘발성 메모리(119)는 신뢰 플랫폼 모듈(100)과 연관된 영속적인 식별자 및 상태를 저장한다. 이때 비휘발성 메모리(119)는 정적 데이터 항목을 저장할 수 있지만, 사용자가 허가한 개체를 통해 동적 데이터 항목을 저장할 수도 있다.

<18> 휘발성 메모리(121)는 동적 데이터 항목을 저장한다.

<19> 키 저장부(123)는 다른 장치를 인증하기 위한 암호화 키 또는 다른 장치와 통신하기 위한 암호화 키를 저장한다.

<20> 이와 같은 종래의 신뢰 플랫폼 모듈은 부팅 코드, 디바이스 드라이버 등이 칩으로 제작되면 변경이 불가능하여 기능이 한정되는 문제점이 있었다.

발명의 내용

해결 하고자하는 과제

<21> 본 발명이 이루고자 하는 기술적 과제는 모바일 디바이스의 무결성을 보장하고, 안전한 키의 생성과 저장된 데이터를 보호하는 모바일용 플랫폼 장착용 모듈을 제공하는 것이다. 또한 기능 변경이 용이한 모바일용 플랫폼 장착용 모듈을 제공하는 것이다.

과제 해결수단

<22> 본 발명의 특징에 따른 플랫폼 장착용 모듈은 입출력 인터페이스부, 실행 엔진부, 무결성 검사부, 키 생성부, 암호화 엔진부, 휘발성 메모리부, 실난수 생성부, 오류 검출부 및 비휘발성 메모리부를 포함한다. 입출력 인터페이스부는 모바일 디바이스와 통신을 위한 인터페이스를 제공한다. 실행 엔진부 미리 저장된 제1 코드에 대응하는 펌웨어를 실행하여 데이터를 생성한다. 무결성 검사부는 해시 연산을 통해 인증 절차를 수행하여 무결성을 보장한다. 키 생성부는 대칭키 쌍 및 알에스에이 암호화 방식에 대응하는 암호키 쌍을 생성한다. 암호화 엔진부는 암호키 쌍을 이용하여 데이터를 암호화하여 암호화된 데이터를 생성한다. 휘발성 메모리부는 동적 데이터를 저장한다. 실난수 생성부는 임의의 연속적인 수에 해당하는 난수를 생성한다. 물리적 오류 검출부는 입출력 인터페이스부를 통한 물리적 오류를 검출하여 물리적 오류에 대응하는 리셋 신호를 생성한다. 비휘발성 메모리부는 제1 코드를 저장하고, 입출력 인터페이스부를 통해 모드 선택 신호를 수신하여 모드 선택 신호를 바탕으로 실행 엔진부로 제1 코드 이외의 코드를 제공한다.

<23> 이때 비휘발성 메모리부는 외부 메모리 제어부, 내부 메모리 제어부 및 모드 입출력 제어부를 포함한다. 외부 메모리 제어부는 입출력 인터페이스부를 통해 모바일 디바이스에 해당하는 외부 메모리와 통신하고, 실행 엔진부와 통신한다. 비휘발성 메모리는 전원이 공급되지 않아도 저장된 정보를 계속 유지하며, 제1 코드, 암호화된 데이터, 대칭키 쌍 및 암호키 쌍을 저장한다. 내부 메모리 제어부는 비휘발성 메모리를 제어하고, 실행 엔진부와 통신한다. 모드 입출력 제어부는 모드 선택 신호에 따라 외부 메모리 제어부 및 내부 메모리 제어부를 제어한다.

<24> 또한 키 생성부는 키 생성 제어부, 소수 생성부 및 암호키 생성부를 포함한다. 키 생성 제어부는 키 생성 코드에 따라 키 생성 제어 신호를 생성한다. 소수 생성부는 난수를 바탕으로 키 생성 제어 신호에 따라 소수 쌍을 생성한다. 암호키 생성부는 소수 쌍을 바탕으로 공개 키 및 개인 키를 포함하는 암호키 쌍을 생성한다.

<25> 또한 입출력 인터페이스부는 범용 입출력 모듈, 범용 비동기 송수신 모듈, 투와이어 인터페이스 모듈 및 로컬 입출력 모듈을 포함한다. 범용 입출력 모듈은 일반적인 용도로 사용이 가능한 입출력 모듈에 해당하고, 통상의 입출력 단자를 가진다. 범용 비동기 송수신 모듈은 모뎀 또는 직렬 통신 장치와 통신하여 데이터를 송수신할 수 있는 모듈에 해당하고, 통상의 입출력 단자를 가진다. 투와이어 인터페이스 모듈은 범용 2-핀 직렬 통신 모듈에 해당하고, 통상의 입출력 단자를 가진다. 로컬 입출력 모듈은 비휘발성 메모리부와 모바일 디바이스간의 인터페이스를 제공한다.

<26> 또한 무결성 검사부는 입력 제어부, 해시 연산부 및 출력 제어부를 포함한다. 입력 제어부는 입출력 인터페이스부를 통해 사용자 인증 메시지를 포함하는 사용자 인증 신호를 입력 받는다. 해시 연산부는 사용자 인증 메시지에 대해 해시 연산을 수행하여 사용자 인증 메시지에 대응하는 해시 연산값을 생성한다. 출력 제어부는 해시 연산값이 미리 정해진 값에 대응하는 값인지를 검사하고, 검사 결과에 따라 출력을 제어한다.

<27> 또한 암호화 엔진부는 데이터 입출력부, 데이터 임시저장부, 알에스에이 연산부 및 중간값 저장부를 포함한다. 데이터 입출력부는 암호화 엔진부의 입력 데이터 및 출력 데이터를 처리한다. 데이터 임시저장부는 입력 데이터 및 출력 데이터를 임시 저장한다. 알에스에이 연산부는 비트 가변적인 처리 구조를 가지고, 알에스에이 암호화 연산을 수행한다. 중간값 저장부는 알에스에이 연산부가 생성하는 중간 데이터 값을 저장한다.

<28> 또한 실난수 생성부는 난수 생성 제어부, 시드 생성부 및 난수 발생부를 포함한다. 난수 생성 제어부는 난수가 필요한 경우 난수를 생성하기 위한 난수 생성 제어 신호를 생성한다. 시드 생성부는 난수 생성 제어 신호에 따라 시드를 생성한다. 난수 발생부는 시드를 바탕으로 난수를 발생시킨다.

<29> 또한 물리적 오류 검출부는 온도 감시부, 전압 감시부, 주파수 감시부 및 제어 신호 생성부를 포함한다. 온도 감시부는 플랫폼 장착용 모듈의 내부의 온도를 감시하여 온도가 미리 정해진 허용 온도 범위를 벗어나면, 온도에 대응하는 온도 제어 신호를 생성한다. 전압 감시부는 플랫폼 장착용 모듈에 입력되는 신호의 전압을 감시하

여 전압이 미리 정해진 허용 전압 범위를 벗어나면, 전압에 대응하는 전압 제어 신호를 생성한다. 주파수 감시부는 신호의 주파수를 감시하여 주파수가 미리 정해진 허용 주파수 범위를 벗어나면, 주파수에 대응하는 주파수 제어 신호를 생성한다. 제어 신호 생성부는 온도 제어 신호, 전압 제어 신호 또는 주파수 제어 신호를 바탕으로 플랫폼 장착용 모듈의 내부에서 실행 중인 동작을 중지시키고, 동작 중에 생성된 결과를 초기화 시키는 리셋 신호를 생성한다.

<30> 또한 제어 신호 생성부는 플랫폼 장착용 모듈의 클럭 및 전원을 차단시키는 리셋 신호를 생성한다.

<31> 본 발명의 다른 특징에 따른 기능 변경 방법은 입출력 인터페이스부, 제1 코드를 저장하는 내부 메모리 및 제1 코드에 대응하는 펌웨어를 실행하는 실행 엔진을 포함하는 플랫폼 장착용 모듈을 위한 기능 변경 방법으로서, 플랫폼 장착용 모듈은 입출력 인터페이스부를 통해 제2 코드가 저장된 외부 메모리 또는 제3 코드가 저장된 모바일 장치와 통신하며, 기능 변경 방법은 입출력 인터페이스부를 통해 모드 선택 정보 및 메모리 선택 정보를 포함하는 모드 선택 신호를 수신하는 단계, 모드 선택 정보에 따라 갱신 모드를 실행하는 경우, 모바일 장치로부터 제3 코드를 수신하는 단계, 그리고 메모리 선택 정보에 따라 내부 메모리에 저장된 코드를 갱신하는 경우, 내부 메모리에 저장된 제1 코드를 제3 코드로 갱신하는 단계를 포함한다.

<32> 이때 기능 변경 방법은 메모리 선택 정보에 따라 외부 메모리에 저장된 코드를 갱신하는 경우, 입출력 인터페이스부를 이용하여 외부 메모리에 저장된 제2 코드를 제3 코드로 갱신하는 단계를 더 포함한다.

<33> 또한 기능 변경 방법은 모드 선택 정보 및 메모리 선택 정보에 따라 외부 메모리에 저장된 코드를 실행하는 경우, 외부 메모리에 저장된 제2 코드를 실행 엔진으로 전달하여 실행 엔진이 제2 코드를 실행하도록 하는 단계를 더 포함한다.

<34> 또한 기능 변경 방법은 모드 선택 정보 및 메모리 선택 정보에 따라 내부 메모리에 저장된 코드를 실행하는 경우, 제3 코드를 수신하는 단계 이전에 내부 메모리에 저장된 제1 코드를 실행 엔진으로 전달하여 실행 엔진이 제1 코드를 실행하도록 하는 단계를 더 포함한다.

효 과

<35> 본 발명의 특징에 따르는 플랫폼 장착용 모듈은 저장된 데이터를 보호하여 모바일 디바이스의 무결성을 보장하고, 모바일 디바이스의 외부로부터 코드를 입력받을 수 있는 구조를 통해 플랫폼 장착용 모듈의 기능을 변경할 수 있다.

발명의 실시를 위한 구체적인 내용

<36> 아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

<37> 명세서 전체에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다. 또한, 명세서에 기재된 "…부", "…기", "모듈" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어나 소프트웨어 또는 하드웨어 및 소프트웨어의 결합으로 구현될 수 있다.

<38> 이제 도면을 참고하여 본 발명의 실시예에 따른 플랫폼 장착용 모듈 및 플랫폼 장착용 모듈을 위한 기능 변경 방법에 대해 설명한다.

<39> 먼저 도 2를 참고하여 본 발명의 실시예에 따른 모바일용 신뢰 플랫폼 모듈에 대해 설명한다.

<40> 도 2는 본 발명의 실시예에 따른 모바일용 신뢰 플랫폼 모듈의 구성을 도시한 도면이다.

<41> 도 2에 도시된 바와 같이, 본 발명의 실시예에 따른 모바일용 신뢰 플랫폼 모듈(200)은 입출력 인터페이스부(210), 실행 엔진부(220), 무결성 검사부(230), 실난수 생성부(240), 키 생성부(250), 알에스에이 엔진부(Rivest Shamir Adleman 엔진부, 이하에서는 'RSA 엔진부'라고도 함)(260), 전압/온도/주파수 검출부(이하에서는 'VTF 검출부'라고도 함)(270), 비휘발성 메모리부(280) 및 휘발성 메모리부(290)를 포함한다.

<42> 입출력 인터페이스부(210)는 모바일용 신뢰 플랫폼 모듈(200)의 외부의 모바일 디바이스와의 인터페이스를 제공

한다. 이때 입출력 인터페이스부(210)는 다양한 프로토콜을 구현하여 다양한 디바이스(Mobile Device)와의 인터페이스를 제공할 수 있다.

<43> 실행 엔진부(220)는 미리 저장된 코드에 대응하는 펌웨어를 실행하여, 펌웨어에 대응하는 데이터를 생성한다. 이때 실행 엔진부(220)는 미리 저장된 코드에 따라 특정 기능만을 수행하고, 코드를 저장하기 위한 메모리를 제어할 수 있다. 또한 실행 엔진부(220)는 모바일용 신뢰 플랫폼 모듈(200)의 사용자의 명령에 따라 실행 엔진부(220)의 외부로부터 코드를 전달 받아, 전달된 코드에 대응하는 펌웨어를 실행할 수도 있다.

<44> 무결성 검사부(230)는 모바일용 신뢰 플랫폼 모듈(200)에 대한 무결성 검사를 수행하여 모바일용 신뢰 플랫폼 모듈(200)의 무결성을 보장한다. 이때 무결성 검사부(230)는 해시(Hash) 연산과 메시지 인증 코드 생성을 통해 디바이스 및 사용자 인증 절차를 수행하여, 모바일용 신뢰 플랫폼 모듈(200)의 무결성을 보장할 수 있다.

<45> 실난수 생성부(240)는 키 또는 다른 값 등의 계산에 초기 값을 제공하기 위한 임의의 연속적인 수에 해당하는 난수를 생성한다.

<46> 키 생성부(250)는 실난수 생성부(240)가 생성한 난수를 바탕으로 암호화 또는 복호화를 위한 대칭키 쌍 및 RSA 암호키 쌍을 생성한다. 이때 RSA 암호키 쌍은 공개 키(Public Key) 및 개인 키(Private Key)를 포함한다.

<47> RSA 엔진부(260)는 키 생성부(250)가 생성한 RSA 암호키 쌍을 이용하여 암호화 또는 복호화를 수행한다.

<48> VTF 검출부(270)는 모바일용 신뢰 플랫폼 모듈(200)의 외부로부터 전압, 온도 및 동작 주파수 변경과 같은 물리적 오류 주입 공격을 당하는 경우, 이와 같은 물리적 오류를 검출하여 모바일용 신뢰 플랫폼 모듈(200)의 동작을 차단하고, 동작 중에 생성된 내부의 데이터를 초기화시키기 위한 리셋 신호를 생성한다.

<49> 비휘발성 메모리부(280)는 실행 엔진부(220)가 실행할 코드 및 키 생성부(250)가 생성하는 RSA 암호키 쌍 등을 저장한다. 이때 비휘발성 메모리부(280)는 입출력 인터페이스부(210)를 통해 외부로부터 실행 엔진부(220)가 실행할 코드를 수신할 수 있다.

<50> 휘발성 메모리부(290)는 실행 엔진부(220)의 동작에 따라 발생하는 동적 데이터를 저장한다.

<51> 다음은 도 3을 참고하여 본 발명의 실시예에 따른 모바일용 신뢰 플랫폼 모듈의 입출력 인터페이스부에 대해 설명한다.

<52> 도 3은 본 발명의 실시예에 따른 입출력 인터페이스부의 구성을 도시한 도면이다.

<53> 도 3에 도시된 바와 같이, 본 발명의 실시예에 따른 입출력 인터페이스부(210)는 범용 입출력 모듈(General Purpose Input/Output Module, 이하에서는 'GPIO 모듈'이라고도 함)(211), 범용 비동기 송수신 모듈(Universal Asynchronous Receiver/Transmitter Module, 이하에서는 'UART 모듈'이라고도 함)(213), 투와이어 인터페이스 모듈(Two Wire Interface Module, 이하에서는 'TWI 모듈'이라고도 함)(215), 로컬 입출력 모듈(Local Input/Output Module, 이하에서는 'LIO 모듈'이라고도 함)(217) 및 입출력 제어부(219)를 포함한다.

<54> GPIO 모듈(211)은 일반적인 용도로 사용이 가능한 입출력 모듈이고, 통상의 입출력 단자를 가질 수 있다.

<55> UART 모듈(213)은 모뎀 또는 직렬 통신 장치와 통신하여 데이터를 송수신할 수 있는 모듈이고, 통상의 입출력 단자를 가질 수 있다.

<56> TWI 모듈(215)은 범용 2-핀 직렬 통신 모듈이고, 통상의 입출력 단자를 가질 수 있다.

<57> LIO 모듈(217)은 비휘발성 메모리부(280)와 모바일용 신뢰 플랫폼 모듈(200)의 외부의 디바이스간의 인터페이스를 제공한다.

<58> 입출력 제어부(219)는 GPIO 모듈(211), UART 모듈(213), TWI 모듈(215) 및 LIO 모듈(217)의 각각에 대한 프로토콜을 구현하여, 모바일용 신뢰 플랫폼 모듈(200)과 모바일용 신뢰 플랫폼 모듈(200)의 외부의 디바이스간의 인터페이스를 제공하고, 모바일용 신뢰 플랫폼 모듈(200)의 입출력을 제어한다.

<59> 다음은 도 4를 참고하여 본 발명의 실시예에 따른 모바일용 신뢰 플랫폼 모듈의 무결성 검사부에 대해 설명한다.

<60> 도 4는 본 발명의 실시예에 따른 무결성 검사부의 구성을 도시한 도면이다.

<61> 도 4에 도시된 바와 같이, 본 발명의 실시예에 따른 무결성 검사부(230)는 입력 제어부(231), 해시 연산부(233) 및 출력 제어부(235)를 포함한다.

<62> 입력 제어부(231)는 사용자 인증 메시지와 같은 메시지가 포함된 신호를 입력받아, 입력된 신호에 포함된 메시지를 해시 연산부(233)에 전달한다.

<63> 해시 연산부(233)는 입력 제어부(231)로부터 전달받은 메시지에 대해 해시 연산을 수행하여, 메시지에 대응하는 해시 연산값을 생성한다. 이때 해시 연산부(233)는 안전한 해시 알고리즘-1(Secure Hash Algorithm-1, 이하에서는 'SHA-1'이라고도 함) 또는 해시 기반 메시지 인증 코드(keyed-Hash for Message Authentication Code, 이하에서는 'HMAC'이라고도 함)를 통해 해시 연산을 수행할 수 있다.

<64> 출력 제어부(235)는 해시 연산값이 미리 정해진 값에 대응하는 값인지를 검사하고, 출력을 제어한다.

<65> 다음은 도 5를 참고하여 본 발명의 실시예에 따른 모바일용 신뢰 플랫폼 모듈의 실난수 생성부에 대해 설명한다.

<66> 도 5는 본 발명의 실시예에 따른 실난수 생성부의 구성을 도시한 도면이다.

<67> 도 5에 도시된 바와 같이, 본 발명의 실시예에 따른 실난수 생성부(240)는 난수 생성 제어부(241), 시드 생성부(243) 및 난수 발생부(245)를 포함한다.

<68> 난수 생성 제어부(241)는 난수가 필요한 경우 난수를 생성하기 위한 난수 생성 제어 신호를 통해 시드 생성부(243)를 제어한다.

<69> 시드 생성부(243)는 난수 생성 제어부(241)의 난수 생성 제어 신호에 따라 시드(seed)를 생성하여 시드에 대응하는 데이터 및 클럭을 출력한다.

<70> 난수 발생부(245)는 시드 생성부(243)가 출력하는 시드에 대응하는 데이터 및 클럭을 바탕으로 난수를 발생시킨다.

<71> 다음은 도 6을 참고하여 본 발명의 실시예에 따른 모바일용 신뢰 플랫폼 모듈의 키 생성부에 대해 설명한다.

<72> 도 6은 본 발명의 실시예에 따른 키 생성부의 구성을 도시한 도면이다.

<73> 도 6에 도시된 바와 같이, 본 발명의 실시예에 따른 키 생성부(250)는 키 생성 제어부(251), 키 생성 코드 저장부(253), 소수 생성부(255) 및 암호키 생성부(257)를 포함한다.

<74> 키 생성 제어부(251)는 미리 정해진 키 생성 절차에 해당하는 키 생성 코드에 따라 키 생성 제어 신호를 생성하여, 키 생성 제어 신호를 통해 키 생성부(250)를 제어하고, 입력 데이터 및 출력 데이터를 처리한다.

<75> 키 생성 코드 저장부(253)는 비대칭 키 쌍을 생성하는 키 생성 절차에 해당하는 키 생성 코드를 저장한다.

<76> 소수 생성부(255)는 실난수 생성부(240)가 생성한 난수를 바탕으로 키 생성 제어부(251)의 키 생성 제어 신호에 따라 소수 쌍을 생성한다. 이때 소수 생성부(255)는 실난수 생성부(240)에서 생성된 난수를 바탕으로 RSA 엔진부(260)의 RSA 암호화 연산을 이용하여 생성된 소수 쌍에 대해 확정적 소수 여부를 판정할 수 있다. 또한 소수 생성부(255)는 모듈러 지수승 연산을 통해 확정적 소수 여부를 판정할 수도 있다.

<77> 암호키 생성부(257)는 소수 생성부(255)가 생성한 소수 쌍을 바탕으로 공개 키 및 개인 키를 포함하는 RSA 암호키 쌍을 생성한다. 이때 암호키 생성부(257)는 소수 쌍을 바탕으로 유클리드 호제법을 이용하여 모듈러스 및 공개키 쌍을 생성한 후, 모듈러스 및 공개키 쌍을 바탕으로 공개 키 및 개인 키를 생성할 수 있다.

<78> 다음은 도 7을 참고하여 본 발명의 실시예에 따른 모바일용 신뢰 플랫폼 모듈의 RSA 엔진부에 대해 설명한다.

<79> 도 7은 본 발명의 실시예에 따른 RSA 엔진부의 구성을 도시한 도면이다.

<80> 도 7에 도시된 바와 같이, 본 발명의 실시예에 따른 RSA 엔진부(260)는 데이터 임시저장부(261), 데이터 입출력부(263), 중간값 저장부(265), RSA 연산부(267) 및 입출력 제어부(269)를 포함한다.

<81> 데이터 임시저장부(261)는 1Kbit/32bit 출력의 램(RAM) 모듈로 RSA 암호화 연산을 위한 입력 및 출력 데이터를 임시 저장한다.

<82> 데이터 입출력부(263)는 데이터 임시저장부(261), 중간값 저장부(265) 및 입출력 제어부(269)의 각각에 데이터 입력 및 출력을 처리한다.

<83> 중간값 저장부(265)는 RSA 연산부(267)의 연산에 필요한 입력 데이터를 제공하고, RSA 연산부(267)가 생성하는 중간 데이터 값을 저장한다.

<84> RSA 연산부(267)는 비트 가변적인 처리 구조로 RSA 암호화 연산을 수행한다. 이때 RSA 연산부(267)는 256비트, 512비트, 1024비트 또는 2048비트를 처리할 수 있는 비트 가변적인 처리 구조를 가질 수 있다. 또한 RSA 연산부(267)는 RSA 암호키 쌍을 이용하여 RSA 암호화 연산을 수행할 수 있다.

<85> 입출력 제어부(269)는 입출력 인터페이스를 수행한다.

<86> 다음은 도 8을 참고하여 본 발명의 실시예에 따른 모바일용 신뢰 플랫폼 모듈의 VTF 검출부에 대해 설명한다.

<87> 도 8은 본 발명의 실시예에 따른 VTF 검출부의 구성을 도시한 도면이다.

<88> 도 8에 도시된 바와 같이, 본 발명의 실시예에 따른 VTF 검출부(270)는 온도 감시부(271), 전압 감시부(273), 주파수 감시부(275) 및 제어 신호 생성부(277)를 포함한다.

<89> 온도 감시부(271)는 모바일용 신뢰 플랫폼 모듈(200)의 내부의 온도를 감시하여, 모바일용 신뢰 플랫폼 모듈(200)의 내부의 온도가 미리 정해진 허용 온도 범위를 벗어나는 경우, 모바일용 신뢰 플랫폼 모듈(200)의 내부의 온도가 허용 온도 범위를 벗어났음을 알리는 온도 제어 신호를 생성한다.

<90> 전압 감시부(273)는 모바일용 신뢰 플랫폼 모듈(200)에 입력되는 신호의 전압을 감시하여, 입력된 신호의 전압이 미리 정해진 허용 전압 범위를 벗어나는 경우, 입력된 신호의 전압이 허용 전압 범위를 벗어났음을 알리는 전압 제어 신호를 생성한다.

<91> 주파수 감시부(275)는 모바일용 신뢰 플랫폼 모듈(200)에 입력되는 신호의 주파수를 감시하여, 입력된 신호의 주파수가 미리 정해진 허용 주파수 범위를 벗어나는 경우, 입력된 신호의 주파수가 허용 주파수 범위를 벗어났음을 알리는 주파수 제어 신호를 생성한다.

<92> 제어 신호 생성부(277)는 온도 제어 신호, 전압 제어 신호 또는 주파수 제어 신호를 바탕으로 모바일용 신뢰 플랫폼 모듈(200)의 내부에서 실행 중인 동작을 중지시키고 동작 중에 생성된 결과를 초기화 시키는 리셋 신호를 생성한다.

<93> 이때 제어 신호 생성부(277)는 모바일용 신뢰 플랫폼 모듈의 내부의 클럭을 초기화 시키는 클럭 리셋 신호를 생성할 수 있고, 모바일용 신뢰 플랫폼 모듈의 내부의 클럭 및 전원을 차단시키는 전원 리셋 신호를 생성할 수도 있다.

<94> 다음은 도 9를 참고하여 본 발명의 실시예에 따른 모바일용 신뢰 플랫폼 모듈의 비휘발성 메모리부에 대해 설명한다.

<95> 도 9는 본 발명의 실시예에 따른 비휘발성 메모리부의 구성을 도시한 도면이다.

<96> 도 9에 도시된 바와 같이, 본 발명의 실시예에 따른 비휘발성 메모리부(280)는 모드 입출력 제어부(281), 외부 메모리 제어부(283), 내부 메모리 제어부(285) 및 비휘발성 메모리(287)를 포함한다.

<97> 모드 입출력 제어부(281)는 입출력 인터페이스부(210)를 통해 모바일용 신뢰 플랫폼 모듈(200)의 사용자로부터 모드 선택 신호를 입력 받아, 모드 선택 신호를 바탕으로 외부 메모리 제어부(283) 또는 내부 메모리 제어부(285)를 제어한다.

<98> 이때 모드 선택 신호는 모드 선택 정보를 포함하고, 모드 입출력 제어부(281)는 모드 선택 정보에 따라 갱신 모드 또는 실행 모드 중 어느 하나의 모드를 실행할 수 있다.

<99> 또한 모드 선택 신호는 메모리 선택 정보를 더 포함할 수 있고, 모드 입출력 제어부(281)는 메모리 선택 정보에 따라 모바일용 신뢰 플랫폼 모듈(200)의 외부의 메모리(이하에서는 '외부 메모리'라고도 함) 또는 모바일용 신뢰 플랫폼 모듈(200)의 내부의 메모리(이하에서는 '내부 메모리'라고도 함) 중 하나를 선택할 수 있다.

<100> 외부 메모리 제어부(283)는 모드 입출력 제어부(281)의 제어에 따라 입출력 인터페이스부(210)를 통해 외부 메모리와 통신하여, 외부 메모리로부터 데이터를 수신하거나 외부 메모리에 데이터를 저장한다. 이때 외부 메모리 제어부(283)는 실행 엔진부(220)로 데이터를 전달할 수 있고, 실행 엔진부(220)로부터 데이터를 전달받을 수 있다. 또한 외부 메모리 제어부(283)는 플래시(Flash) 메모리 등과 같은 외부 메모리와 통신할 수 있다.

<101> 내부 메모리 제어부(285)는 모드 입출력 제어부(281)의 제어에 따라 내부 메모리로부터 데이터를 불러오거나 내부 메모리에 데이터를 저장한다. 이때 내부 메모리 제어부(285)는 실행 엔진부(220)로 데이터를 전달할 수 있고, 실행 엔진부(220)로부터 데이터를 전달받을 수 있다.

<102> 비휘발성 메모리(287)는 내부 메모리에 해당하고, 전원이 공급되지 않아도 저장된 정보를 계속 유지하는 메모리로서 실행 엔진부(220)가 생성하는 데이터를 저장한다. 이때 비휘발성 메모리(287)는 실행 엔진부(220)가 실행하는 코드, 무결성 검사부(230)가 생성하는 각 구성요소의 무결성 측정값 및 키 생성부(250)가 생성하는 RSA 암호키 쌍 등을 저장할 수 있다. 또한 비휘발성 메모리(287)는 이이피롬(Electrically Erasable and Programmable Read Only Memory, EEPROM) 등에 해당할 수 있다.

<103> 다음은 도 10을 참고하여 본 발명의 실시예에 따른 모바일용 신뢰 플랫폼 모듈을 위한 기능 변경 방법에 대해 설명한다.

<104> 도 10은 본 발명의 실시예에 따른 모바일용 신뢰 플랫폼 모듈을 위한 기능 변경 방법을 도시한 도면이다.

<105> 이때 비휘발성 메모리(287)는 제1 코드를 저장하고, 입출력 인터페이스부(210)를 통해 모바일용 신뢰 플랫폼 모듈(200)과 연결된 플래시 메모리는 제2 코드를 저장한다. 또한 입출력 인터페이스부(210)를 통해 모바일용 신뢰 플랫폼 모듈(200)과 연결된 모바일 장치는 제3 코드를 저장한다.

<106> 도 10에 도시된 바와 같이, 먼저, 모드 입출력 제어부(281)는 입출력 인터페이스부(210)를 통해 모드 선택 신호를 수신한다(S101). 이때 모드 선택 신호는 모드 선택 정보 및 메모리 선택 정보를 포함한다.

<107> 다음, 모드 입출력 제어부(281)는 모드 선택 정보에 따라 갱신 모드 또는 실행 모드 중 하나의 모드를 선택하여, 선택한 모드를 실행한다(S103).

<108> 만약, 갱신 모드를 실행하는 경우, 모드 입출력 제어부(281)는 입출력 인터페이스부(210)를 통해 모바일용 신뢰 플랫폼 모듈(200)과 연결된 모바일 장치로부터 제3 코드를 수신한다(S105).

<109> 다음, 모드 입출력 제어부(281)는 메모리 선택 정보에 따라 코드를 갱신할 메모리를 선택한다(S107).

<110> 만약, 내부 메모리를 선택하는 경우, 모드 입출력 제어부(281)는 내부 메모리 제어부(285)로 코드 갱신 제어 메시지 및 제3 코드를 전달한다(S109).

<111> 다음, 내부 메모리 제어부(285)는 코드 갱신 제어 메시지에 따라 내부 메모리에 해당하는 비휘발성 메모리(287)에 저장된 제1 코드를 제3 코드로 갱신한다(S111).

<112> 한편, 외부 메모리를 선택하는 경우, 모드 입출력 제어부(281)는 외부 메모리 제어부(283)로 코드 갱신 제어 메시지 및 제3 코드를 전달한다(S113).

<113> 다음, 외부 메모리 제어부(283)는 코드 갱신 제어 메시지에 따라 입출력 인터페이스부(210)를 통해 외부 메모리에 해당하는 플래시 메모리에 저장된 제2 코드를 제3 코드로 갱신한다(S115).

<114> 한편, 실행 모드를 실행하는 경우, 모드 입출력 제어부(281)는 메모리 선택 정보에 따라 실행할 코드가 저장된 메모리를 선택한다(S117).

<115> 만약, 외부 메모리를 선택하는 경우, 모드 입출력 제어부(281)는 외부 메모리 제어부(283)로 코드 실행 제어 메시지를 전달한다(S119).

<116> 다음, 외부 메모리 제어부(283)는 코드 실행 제어 메시지에 따라 입출력 인터페이스부(210)를 통해 외부 메모리에 해당하는 플래시 메모리로부터 제2 코드를 수신한다(S121).

<117> 이후, 외부 메모리 제어부(283)는 실행 엔진부(220)로 제2 코드를 전달한다(S123).

<118> 다음, 실행 엔진부(220)는 제2 코드에 대응하는 펌웨어를 실행한다(S125).

<119> 한편, 내부 메모리를 선택하는 경우, 모드 입출력 제어부(281)는 내부 메모리 제어부(285)로 코드 실행 제어 메시지를 전달한다(S127).

<120> 다음, 내부 메모리 제어부(285)는 코드 실행 제어 메시지에 따라 내부 메모리에 해당하는 비휘발성 메모리(287)에 저장된 제1 코드를 실행 엔진부(220)로 전달한다(S129).

<121> 이후, 실행 엔진부(220)는 제1 코드에 대응하는 펌웨어를 실행한다(S131).

<122> 이를 통해 모바일용 신뢰 플랫폼 모듈은 미리 저장된 코드를 갱신할 수 있고, 사용자의 선택에 따라 미리 정해진 펌웨어와 다른 펌웨어를 실행하여 기능을 변경할 수도 있다.

<123> 이상에서 설명한 본 발명의 실시예는 장치 및 방법을 통해서만 구현이 되는 것은 아니며, 본 발명의 실시예의

구성에 대응하는 기능을 실현하는 프로그램 또는 그 프로그램이 기록된 기록 매체를 통해 구현될 수도 있으며, 이러한 구현은 앞서 설명한 실시예의 기재로부터 본 발명이 속하는 기술분야의 전문가라면 쉽게 구현할 수 있는 것이다.

<124> 이상에서 본 발명의 실시예에 대하여 상세하게 설명하였지만 본 발명의 권리범위는 이에 한정되는 것은 아니고 다음의 청구범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 발명의 권리범위에 속하는 것이다.

도면의 간단한 설명

<125> 도 1은 종래의 신뢰 플랫폼 모듈의 구성을 도시한 도면이다.

<126> 도 2는 본 발명의 실시예에 따른 모바일용 신뢰 플랫폼 모듈의 구성을 도시한 도면이다.

<127> 도 3은 본 발명의 실시예에 따른 입출력 인터페이스부의 구성을 도시한 도면이다.

<128> 도 4는 본 발명의 실시예에 따른 무결성 검사부의 구성을 도시한 도면이다.

<129> 도 5는 본 발명의 실시예에 따른 실난수 생성부의 구성을 도시한 도면이다.

<130> 도 6은 본 발명의 실시예에 따른 키 생성부의 구성을 도시한 도면이다.

<131> 도 7은 본 발명의 실시예에 따른 RSA 엔진부의 구성을 도시한 도면이다.

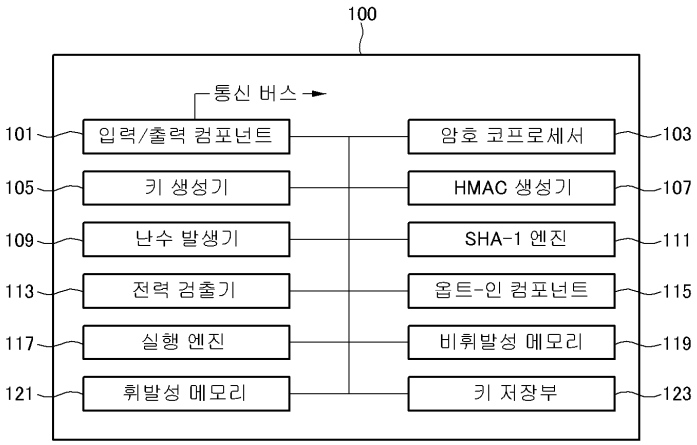
<132> 도 8은 본 발명의 실시예에 따른 VTF 검출부의 구성을 도시한 도면이다.

<133> 도 9는 본 발명의 실시예에 따른 비휘발성 메모리부의 구성을 도시한 도면이다.

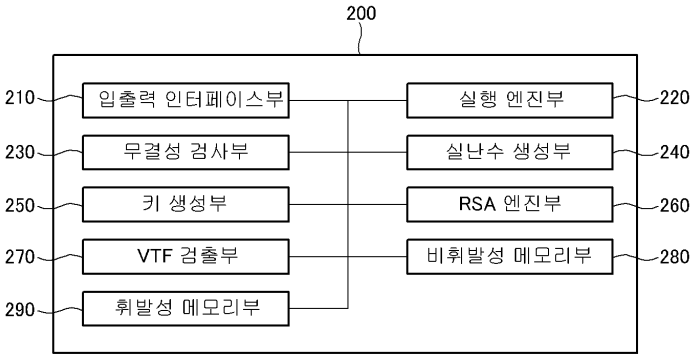
<134> 도 10은 본 발명의 실시예에 따른 모바일용 신뢰 플랫폼 모듈을 위한 기능 변경 방법을 도시한 도면이다.

도면

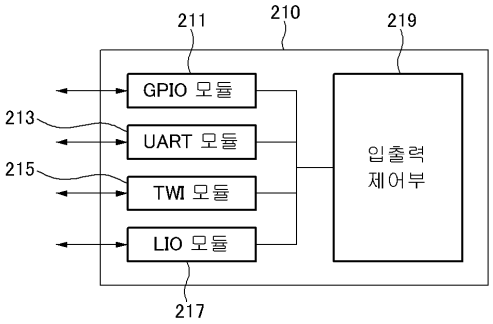
도면1



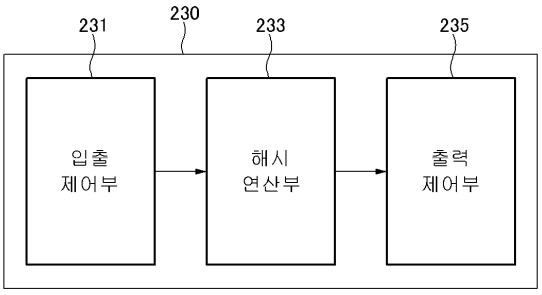
도면2



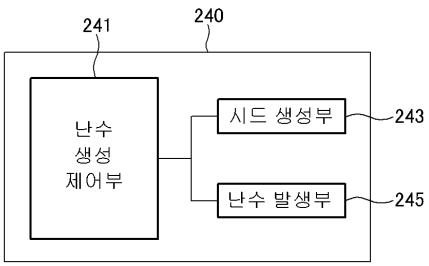
도면3



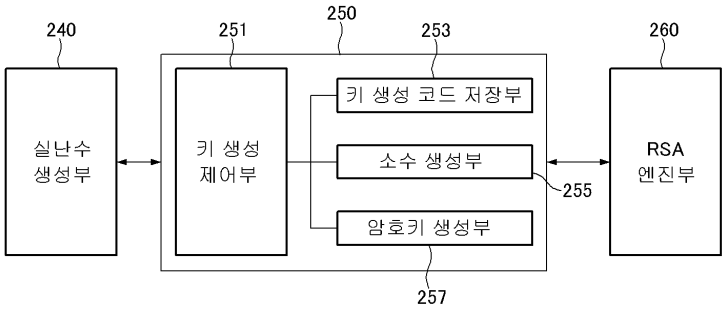
도면4



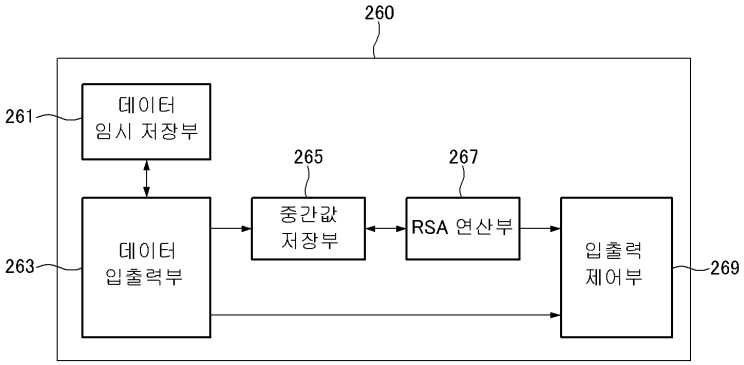
도면5



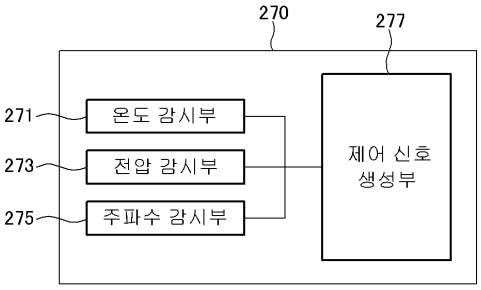
도면6


240
251
250
253
260
실난수
생성부
키 생성
제어부
키 생성 코드 저장부
소수 생성부
255
암호키 생성부
257
RSA
엔진부

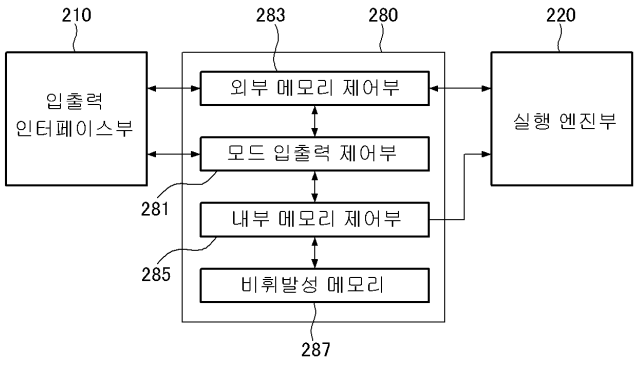
도면7


260
261
데이터
임시 저장부
265
267
중간값
저장부
RSA 연산부
263
데이터
입출력부
입출력
제어부
269

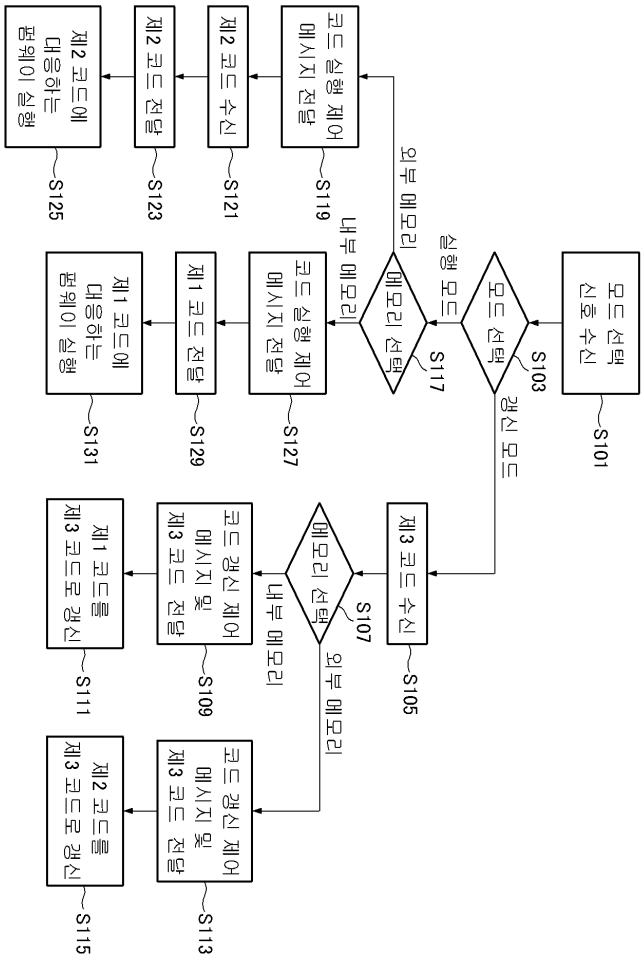
도면8


270
277
271
온도 감시부
273
전압 감시부
275
주파수 감시부
제어 신호
생성부

도면9


210
283
280
220
입출력
인터페이스부
외부 메모리 제어부
모드 입출력 제어부
내부 메모리 제어부
비휘발성 메모리
실행 엔진부
281
285
287

도면10


모드 선택
신호 수신
S101
모드 선택
S103
실행 모드
갱신 모드
메모리 선택
S117
외부 메모리
내부 메모리
코드 실행 제어
메시지 전달
S119
제2 코드 수신
S121
제2 코드 전달
S123
제2 코드에
대응하는
펌웨이 실행
S125
제3 코드 수신
S105
메모리 선택
S107
내부 메모리
외부 메모리
코드 갱신 제어
메시지 및
제3 코드 전달
S109
제1 코드를
제3 코드로 갱신
S111
코드 갱신 제어
메시지 및
제3 코드 전달
S113
제2 코드를
제3 코드로 갱신
S115
코드 실행 제어
메시지 전달
S127
제1 코드 전달
S129
제1 코드에
대응하는
펌웨이 실행
S131