(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl. [7]
G06F 11/00

(11) 공개번호 특2002-0007403
(43) 공개일자 2002년01월26일

(21) 출원번호 10-2001-7014234
(22) 출원일자 2001년11월07일
번역문 제출일자 2001년11월07일
(86) 국제출원번호 PCT/US2000/12479
(86) 국제출원출원일자 2000년05월05일
(87) 국제공개번호 WO 2000/68791
(87) 국제공개일자 2000년11월16일

(81) 지정국 국내특허 : 아랍에미리트, 안티구아바부다, 알바니아, 아르메니아, 오스트리아, 오스트레일리아, 아제르바이잔, 보스니아-헤르체고비나, 바베이도스, 불가리아, 브라질, 벨라루스, 캐나다, 스위스, 중국, 코스타리카, 쿠바, 체코, 독일, 덴마크, 도미니카연방, 알제리, 에스토니아, 스페인, 핀랜드, 영국, 그레나다, 그루지야, 가나, 감비아, 크로아티아, 헝가리, 인도네시아, 이스라엘, 인도, 아이슬란드, 일본, 케냐, 키르기즈, 북한, 대한민국, 카자흐스탄, 세인트루시아, 스리랑카, 라이베리아, 레소토, 리투아니아, 룩셈부르크, 라트비아, 모로코, 몰도바, 마다가스카르, 마케도니아, 몽고, 말라위, 멕시코, 노르웨이, 뉴질랜드, 폴란드, 포르투칼, 루마니아, 러시아, 수단, 스웨덴, 싱가포르, 슬로베니아, 슬로바키아, 시에라리온, 타지키스탄, 투르크메니스탄, 터어키, 트리니다드토바고, 탄자니아, 우크라이나, 우간다, 우즈베키스탄, 베트남, 유고슬라비아, 남아프리카, 짐바브웨,
AP ARIPO특허: 가나, 감비아, 케냐, 레소토, 말라위, 수단, 시에라리온, 스와질랜드, 탄자니아, 우간다, 짐바브웨,
EA 유라시아특허: 아르메니아, 아제르바이잔, 벨라루스, 키르기즈, 카자흐스탄, 몰도바, 러시아, 타지키스탄, 투르크메니스탄,
EP 유럽특허: 오스트리아, 벨기에, 스위스, 사이프러스, 독일, 덴마크, 스페인, 핀랜드, 프랑스, 영국, 그리스, 아일랜드, 이탈리아, 룩셈부르크, 모나코, 네덜란드, 포르투칼, 스웨덴,
OA OAPI특허: 부르키나파소, 베넹, 중앙아프리카, 콩고, 코트디브와르, 카메룬, 가봉, 기네, 기네비쏘, 말리, 모리타니, 니제르, 세네갈, 차드, 토고,

(30) 우선권주장 60/133,131 1999년05월07일 미국(US)

(71) 출원인 모픽스 테크놀로지 아이엔씨
미국, 캘리포니아 95008-0638, 캠프벨, 에스.베스코 애비뉴 1550

(72) 발명자 와슨스테판엘
미국,캘리포니아95006,바울더크릭,알파인드라이브425
반데이비드케이
미국,캘리포니아95128,산호세,박스우드드라이브2445
랄스톤존디
미국,캘리포니아94028,포톨라밸리,라쿠에스타드라이브369

(74) 대리인 허상훈

심사청구 : 없음

(54) 프로그래머블 보안 프로세서 장치 및 방법

요약

디지털 로직 장치는 인가된 구성 보안 키(538)의 세트를 저장하는 프로그래머블 보안 회로를 구비한다. 보안 회로는 인가 구성 키(360)를 들어오는 구성 요청과 비교하고, 프로그래머블 로직 장치에 대한 새로운 구성(544)를 선택적으로 인에이블시킨다.

대표도

도 5

색인어

프로그래머블 재구성가능한 보안 프로세서, 구성 기능부, 프로파일링/맵핑 분석, 처리 커널, DSP, 제어 마이크로프로세서, 커널 통신 신호, 데이터 라우터, 통신 버스, 커널 제어, 시퀀싱

명세서

기술분야

본 발명은 총체적으로 통신 시스템에 관한 것이다. 보다 상세하게는, 본 발명은 전자 통신 장치용 프로그래머블 재구성가능한 보안 프로세서에 관한 것이다.

배경기술

통상적으로, 전자 통신 장치는 단일 표준 또는 어플리케이션에 따라 단일 기능을 수행하도록 설계되어 왔다. 전자 통신 장치의 첨단화가 진행됨에 따라, 다수의 표준 또는 어플리케이션에 따라 다수의 기능을 수행할 수 있는 전자 장치를 설계하는 것이 가능하다. 단일 표준에 따라 수행하는 제품의 라이센싱 또는 인증은, 라이센스가 제품이 팔릴 때 지정될 수 있기 때문에 직선적이다. 다른 말로 표현하면, 적절한 라이센스 또는 인증을 다수의 표준 또는 어플리케이션에 따라 동작하는 장치에 제공하기가 비교적 어렵다.

상기에 비추어, 각각의 표준이 적절한 인증에 따라 실행되는 다수의 표준 또는 어플리케이션에 따라 전자 통신 장치를 동작시키는 메커니즘을 제공하는 것이 극히 바람직할 것이다.

발명의 상세한 설명

본 발명의 한 실시예에서, 프로그래머블 재구성가능한 보안 프로세서(programmable reconfigurable security processor)는 전자 통신 장치를 인에이블시켜, 각각의 표준 또는 어플리케이션이 적절한 인증에 따라 실행되는 다수의 표준에 따라 동작하거나 다수의 어플리케이션을 수용하게 한다. 프로그래머블 재구성가능한 보안 프로세서는 다른 어플리케이션, 알고리즘, 루틴 또는 유틸리티가 실행시 또는 실행 이전에 로드될 수 있는 임의의 장치에서 이용될 수 있다. 예를 들어, 보안 프로세서는 새로운 표준, 어플리케이션, 시스템 업그레이드 및 시험 기간을 인에이블시키는 지적 소유권에 대한 라이센스를 제어하느데 사용될 수 있다. 더우기, 보안 프로세서는 정보 스트림의 실시간 암호화 및/또는 암호해독을 수행할 수 있다. 본 발명의 이와 같은 실시예는 다중 모드 무선 텔레폰, 징보 단말기, 암호장치, 및 이미지 및 멀티미디어 조작 장치와 같은 다중 모드 제품에 성공적으로 이용될 수 있다.

본 발명의 제2 실시예에 따르면, 디지털 로직 회로는 프로그래머블 로직 장치 및 프로그래머블 보안 회로를 구비한다. 프로그래머블 보안 회로는 인가된 구성 보안 키의 세트를 저장한다. 프로그래머블 보안 회로는 인가된 구성 보안 키를 들어오는 구성 요청과 비교하고, 구성 요청에 응답하여 프로그래머블 로직 장치를 위한 새로운 구성을 선택적으로 인에이블시킨다.

다른 실시예에서, 프로그래머블 보안 회로는 또한 인가된 동작 보안 키를 저장한다. 프로그래머블 보안 회로는 인가된 동작 보안 키를 프로그래머블 로직 장치로부터의 들어오는 동작 요청과 비교하고, 동작 요청에 응답해서 프로그래머블 로직 장치 내의 동작을 인에이블시킨다.

도면의 간단한 설명

도 1은 본 발명의 실시예에 따라 네트워크에 걸쳐 보안 알고리즘을 다운로드하기 위한 예시적인 방법을 도시하는 도면.

도 2는 본 발명의 실시예에 따라 네트워크에 걸쳐 보안 알고리즘을 인증, 실행, 테스트 및 다운로드하기 위한 예시적인 프로세스를 도시하는 도면.

도 3은 본 발명의 실시예에 따라 보안 알고리즘의 파라메타를 프로그래머블 재구성가능한 보안 프로세서로 전달하기 위한 예시적인 방법을 도시하는 도면.

도 4A는 보안 또는 암화화 표준의 세트를 분석하기 위한 예시적인 방법을 도시하는 도면.

도 4B는 본 발명의 실시예에 따라 프로그래머블 재구성가능한 보안 프로세서를 포함하는 예시적인 아키텍춰를 도시하는 도면.

도 5는 본 발명의 실시예에 따라 프로그래머블 재구성가능한 보안 프로세서를 설계하기 위해 보안 또는 암호화 표준의 세트를 프로파일링(profiling)하기 위한 예시적인 프로세스를 도시하는 도면.

도 6A는 본 발명의 실시예에 따른 예시적인 커널을 도시하는 도면.

도 6B는 본 발명의 커널에 의해 구현될 수 있는 예시적인 재구성가능한 데이터 처리 아키텍춰를 도시하는 도면.

도 7은 몇가지 종류의 고정 또는 프로그래머블 데이터 프로세서를 위한 특성 에너지 효율 대 유연성을 도시하는 도면.

도 8은 본 발명의 실시예에 따른 프로그래머블 재구성가능한 보안 프로세서를 도시하는 도면.

도 9는 본 발명의 실시예에 따른 예시적인 커널을 도시하는 도면.

도 10은 본 발명의 실시예에 따른 예시적인 커널을 도시하는 도면.

도 11은 본 발명의 실시예에 따른 프로그래머블 보안 회로를 갖는 예시적인 통신 장치를 도시하는 도면.

도 12는 본 발명의 실시예에 따른 예시적인 프로그래머블 보안 회로를 도시하는 도면.

도 13은 본 발명의 실시예에 따른 예시적인 프로세스의 순서도를 도시하는 도면.

실시예

도 1은 서버(112)에 의해 네트워크(120)에 걸쳐 이동 전자 통신 단말기(190)에 보안 알고리즘에 서비스되는 예시적인 방법을 도시한다. 보안 알고리즘은 암호 키(secret key)를 이용한 공용 키 교환 및 데이터 암화화를 포함할 수 있지만 이에 국한되어 있지 않다. 보안 알고리즘은 서버(112)에 의해 발행되고, 네트워크(120)에 걸쳐 통신 링크(130)을 통해 이동 단말기(190) 내의 저장고(repository)(140)에 전달된다. 저장고(140)는 보안 알고리즘의 도달을 이동 단말기(190)에 알린다. 유연성 보안 프레임워크(150)는 보안 알고리즘을 위한 식별 메커니즘을 수립한다. 예시적인 실시예에서, 보안 알고리즘은 보안 알고리즘의 자격 및 유관한 규정 파라메타(regulatory parameters)/명세의 정의를 포함하는 헤더(152)를 구비한다.

보안 알고리즘의 자격은 예를 들어, 개방 표준, 제조자-지정 또는 임의로 분류될 수 있다. 더우기, 자격은 또한 설치 절차(172)를 포함한다. 규정 파라메타/명세는 예를 들어, 보안 알고리즘의 소스 및 부수적인 자격증(170)의 정의를 포함한다. 헤더(152)에 포함된 정보를 사용하여, 설치는 벤더 지정 어플리케이션 프로그램 인터페이스(API) 및 가상 머신 인터페이스(VMI)(180)에 기초하여 진행할 수 있다. VMI는 이용가능한 하드웨어 자원(182)에 대한 반드시 소프트웨어 프로그래머의 인터페이스이다.

도 2는 본 발명의 실시예에 따른 프로세스를 도시한다. 도 2는 사용자(202), 다운로드 프로세스 관리 루틴(204), 인증 펑션수/당사자(authentication function/party)(206), 및 네트워크(208)을 구비한다. 본 예시적인 실시예에서, 사용자(202)는 이동 통신 장치(190)를 구동시킨다. 네트워크(208)는 이용가능한 보안 서비스를 정의한다. 사용자(202)에 의해 제어되는 이동 단말기(190)가 특정 서비스를 요청하면, 네트워크(208)는 인증 목적으로 자신을 식별한다(단계 210A). 만일 이동 단말기(190)가 인증 펑션/당사자(206)에 대해 인증을 요청하면(즉, 트러스트드 제3자, TTP 또는 다른 인증 제공자에 의해), 인증 펑션/당사자(206)에 의해 인증 유효가 이동 단말기(190)에 반환된다)(단계 210B). 다음에 이동 단말기(190)는 그 인증 정보를 네트워크(280)에 송부한다(단계 210B). 다음에, 네트워크(208)는 이동 단말기(190)로부터 자격 설명(capability description)을 요청하고 수신한다(단계 210C). 자격 설명에 응답해서, 네트워크(208)는 적절한 보안 알고리즘을 선택하고, 선택된 보안 알고리즘을 신뢰성있게 전달하는데 필요한 서비스 품질(즉, 비트 에러율)을 포함하는 보안 알고리즘을 이동 단말기(190)에 송신한다. 다음에, 네트워크(208)는 이동 단말기(190)를 지정하고, 이동 단말기(190)는 보안 알고리즘을 다운로드하기 위한 시나리오를 수신한다(단계 210D). 보안 알고리즘은 가능하게 세그멘트 또는 데이터 패킷으로 이동 단말기(190)에 운반된다(단계 210E). 이동 단말기(190)는 테스팅을 수행하여 올바른 운반인지를 확인하고, 테스팅 결과를 다시 네트워크(208)에 보고한다(단계 210E). 이동 단말기(190)는 다음에 다른 레벨의 인증을 요청하고 수신한다(단계 210E). 다음에, 이동 단말기(190)는 보안 알고리즘을 설치하고, 네트워크(208)에 대한 설치는 확인한다(단계 210F). 빌링 협상(billing negotiation)이 처리된다(단계 210F). 만일 설치된 보안 알고리즘이 종료 기능에 영향을 미치는 부수적인 구성요소를 필요로 하면, 이동 단말기(190)는 이와 같은 소프트웨어를 수신하기 위해 인증 펑션/당사자(206)에 키를 송신한다(단계 210F). 부수적인 소프트웨어가 다운로드되고 설치된다(단계 210F). 마지막으로, 보안 알고리즘의 완전한 기능이 이동 단말기(190)에 의해 테스트되고 확인된다(단계 210G).

도 3은 다중 표준 이동 통신 단말기(190) 내의 프로그래머블 재구성가능한 보안 프로세서(350)를 구성하기 위한 예시적인 프로세스는 도시한다. 보안 알고리즘의 다음 수신시에, 보안 알고리즘의 헤더(152)가 처리되어 구성 테이블(320)을 생성한다. 구성 테이블(320)은 특정 보안 자격 및 대응하는 파라메타 및 값을 포함한다. 구성 테이블(320)에 제공된 정보는 이동 통신 단말기의 API 및 VMI를 거쳐 보안 프로세서(350)에 전달된다. 보안 프로세서(350)는 다수의 파라메타화된 하드웨어 데이터 처리 커널(370)을 구비한다. 각 커널(360)의 내용은 구성 테이블(320)내의 정의에 따라 보안 프로세서(350)에 의해 전달된다.

도 4A는 프로그래머블 재구성가능한 보안 프로세서(350)를 위한 구성 알고리즘을 분석하기 위한 예시적인 방법을 도

시한다. 다수의 보안 표준 또는 보안 알고리즘은 컬(410A,410B,410C)로 표시되어 있다. 다양한 표준 또는 알고리즘에 관련된 데이터 처리 함수들은 행(420A,420B,420C)로 표시되어 있다. 보안 표준의 예는 AES,DES,RSA,MISTY 및 IEDA이다. 결과로 나타나는 매트릭스(400)에 기초하여, 프로그래머블 재구성가능한 보안 프로세서(350)는 다양한 보안 알고리즘의 구성 데이터 처리 기능을 구현하도록 설계된다.

도 4B는 다양한 보안 알고리즘의 구성 데이터 처리 기능을 구현하도록 설계된 예시적인 아키텍춰(430)를 도시한다. 아키텍춰(430)는 프로그래머블 재구성가능한 보안 프로세서(350), 소프트웨어 프로그래머블 프로세서(440), 및 통신 버스(434)를 구비한다. 소프트웨어 프로그래머블 프로세서(440)는 디지털 신호 프로세서(DSP)(442), 및 제어 마이크로프로세서(444)를 구비한다. 통신 서버(434)는 제어 프로세서(444), DSP(442), 및 프로그래머블 재구성가능한 보안 프로세서(350)를 링크한다. 통신 버스(434)로부터의 데이터는 프로그래머블 재구성가능한 보안 프로세서(350) 및 소프트웨어 프로그래머블 프로세서(440)에 인가된다. 프로그래머블 재구성가능한 보안 프로세서(350)는 병렬 이종 데이터 프로세서(도시않됨) 또는 커널(360)의 세트를 포함한다. 커널(360)은 연산적으로 집중적인 데이터 처리 기능을 수행하고, 모듈라 비용장 방식으로 선택되고 구성된다. 바람직하게, 각각의 커널(360) 및 그 상호접속부가 신속하게 재구성될 수 있어, 아키텍춰(430)는 하나의 보안 표준, 어플리케이션 또는 서비스를 다른 것으로 신속하게(즉, 밀리초로) 스위치할 수 있게 된다. DSP(442)는 프로그래머블 재구성가능한 보안 프로세서(350)내의 커널(360)에 의해 수행되는 함수에 관련된 연산적으로 집중적인 데이터 처리 기능을 수행한다. 제어 마이크로프로세서(444)는 제어 및 다른 기능을 수행한다.

도 5는 본 발명의 실시예에 따라 프로그래머블 재구성가능한 보안 프로세서(350)를 정의하기 위한 프로세스를 도시한다. 구성 기능부(420)가 프로파일링/맵핑(profiling/mapping) 분석에 인가된다(단계 530). 프로파일링/맵핑 분석은 연산 비용 또는 세기를 결정하기 위해 각각의 구성 기능부(420)를 분석하는 단계를 포함한다. 가장 연산적으로 집중적인 구성 기능은 프로그래머블 재구성가능한 보안 프로세서(350)의 하나 이상의 처리 커널(360)에 맵핑된다. 나머지 기능들은 DSP(442) 및 제어 마이크로프로세서(444)에 맵핑된다. 부수적으로, 프로파일링/맵핑 분석은 커널 통신 신호를 평가하여(단계 542), 재구성가능한 데이터 라우터(538)의 설계를 결정한다. 데이터 라우터(538)는 통신 버스(434)에의 필요한 모든 커널 간 데이터 전송 및 인터페이스에 영향을 미친다. 프로파일링/맵핑은 또한 커널 제어 및 시퀀싱을 평가한다(단계 544).

도 6A는 본 발명의 실시예에 따른 예시적인 커널(360)을 도시한다. 커널(360)은 로컬 메모리(622), 데이터 시퀀서(624), 및 파라메타가능하고 구성가능한 산술 로직 유닛(ALU)(636)을 구비한다. ALU(626)은 필요한 데이터 처리 연산을 수행한다. 로컬 메모리622)는 고속 캐쉬를 제공한다. 데이터 시퀀서(624)는 로컬 메모리(622)와 ALU(626) 간의 데이터 흐름을 관리한다. 데이터는 버스(610)를 거쳐 커널(360) 내/외로 운반된다. 임의의 구성 제어 또는 상태 신호가 버스(612)를 거쳐 커널(360) 내/외로 운반된다. 구성 제어는 내부 테이블(370)에 설명된 파라메타 및 값에 기초한다.

도 6B는 커널(360)을 위한 부수적인 예시적인 구성가능한 아키텍춰를 도시한다. 예를 들어, 네개의 예시적인 구성가능한 아키텍춰: 프로그래머블 기능 유닛(642), 재구성가능한 데이터경로(644), 재구성가능한 산술 회로(646), 및 재구성가능한 제어 회로(648)을 갖는 재구성 로직중의 하나는 하나 이상의 커널(360)에 맵핑될 수 있다.

도 7은 다른 종류의 장치중에서 에너지 효율(밀리와트당 MOPS로 평가) 및 유연성의 비교를 도시한다. 도 7에 도시된 바와 같이, 프로그래머블 재구성가능한 보안 프로세서(350)는 보안 알고리즘의 세트에 기초하여 최적화되기 때문에 에너지 효율에서 두번째로 좋다. 디지털 신호 마이크로프로세서 및 내장된 프로세서들은 명령어 세트 프로그램가능성을 지원하는데 필요한 오버헤드 때문에 그다지 효율적이지 못하다. 프로그래머블 로직 장치(PLD)는 PLD가 일반적인 자

원을 이용하여 미세한 구성을 가능하게 하여야 하기 때문에 가장 비효율적이다. 비록 고정 함수 하드웨어가 가장 효율적이지만, 고정 함수 하드웨어가 유연하지 못하기 때문에 프로그래머블 재구성가능한 보안 프로세서(350)로서 바람직하짐 못하다.

프로그래머블 재구성가능한 보안 프로세서(350)는 다양한 기능을 수행, 예를 들어, (1) 데이터의 암화화/암호해독을 수행하고, (2) 구성 정보의 암호화/암호해독을 수행하는데 이용될 수 있다. 도 8,9 및 10은 제1의 예시적인 기능을 도시하고, 도 11,12 및 13은 제2의 예시적인 기능을 도시한다.

도 8은 프로그래머블 재구성가능한 보안 프로세서(350)를 도시한다. 보안 프로세서(350)는 신호 세트(802,804)에 의해 상호접속되어 있는 다수의 로직 모듈 또는 커널(360A, 360B,360C,360D)를 구비한다. 한 실시예에서, 신호 세트(802)는 한 치수(즉, 수직으로) 인접한 커널(360)을 인에이블시켜 캐스케이드된다. 예를 들어, 커널(360A,360C)이 신호(802A)에 의해 캐스케이드되어, 커널(360A)의 출력이 커널(360C)의 입력이 된다. 유사하게, 커널(360B,360D)이 신호(802B)에 의해 캐스케이드되어, 커널(360B)의 출력이 커널(360D)의 입력이 된다. 다른 실시예에서, 신호 세트(804)는 다른 치수(즉, 수평으로)에 인접한 커널(360)을 인에이블시켜 캐스케이드된다. 예를 들어, 커널(360A,360B)이 신호(804A)에 의해 캐스케이드되어, 커널(360B)의 최상위 스테이지가 커널(360A)의 최하위 스테이지에 전달된다. 유사하게, 커널(360C,360D)이 신호(804B)에 의해 캐스케이드되어, 커널(360D)의 최상위 스테이지가 커널(360C)의 최하위 스테이지에 전달된다. 더우기, 커널(360)은 입력 및 제어 신호(803)에 의해 구성된다. 변형되지 않은 데이터는 신호 세트(806)를 거쳐 커널(360A, 360B)에 인가된다. 이와 같은 변형되지 않은 데이터는 커널(360)에 의해 처리되어 신호 세트(805)를 거쳐 출력한다.

도 9는 커널(360)의 예시적인 실시예를 도시한다. 커널(360)은 암호화/암호해독 라운드(rounds)를 연산하기 위해 극히 최적화된 축고 명령어 세트 연산 소자를 구현한다. 커널(360)은 프로그래머블 마이크로시퀀서(903), 재구성가능한 데이터 변형 유닛(906), 및 피연산자 메모리(908)를 구비한다. 마이크로시퀀서(903)는 분기 명령 및 한정된 수의 입력/출력 기능을 포함하지만 이에 국한되지 않은 극히 축소된 명령어 세트를 실행하도록 설계되어 있다. 마이크로시퀀서(903)는 도 8의 신호(803)의 서브셋인 입력 및 제어 신호(902)에 의해 구성된다. 마이크로시퀀서(903) 명령어 워드는 적어도 피연산자 코드(OP), 분기 조건 필드(BC), 다음 스테이지 필드(NS), 및 출력 함수 필드(OF)를 구비한다. 피연산자 코드(OP)는 실행되고 있는 명령어의 종류를 정의하고, 분기 조건 필드(BC)는 조건이 명령어 실행의 코스를 변경하는지를 결정하고, 다음 스테이지 필드(NS)는 분기 목적지를 결정하고, 출력 함수 필드(OF)는 제어 신호를 재구성가능한 데이터 변형 유닛(906) 및 피연산자 메모리(908)에 보낸다.

재구성가능한 데이터 변형 유닛(906)의 연산은 두개의 메커니즘, 즉 입력 및 제어 신호(902) 및 시퀀스 제어 신호(904)에 의해 제어된다. 실행이전에, 입력 및 제어 신호(902)는 연산 동안 사룔될 연산 및 상수를 구성한다. 실행 동안, 마이크로시퀀서(903)으로부터의 시퀀스 제어 신호(904)는 마이크로-연산 시퀀스를 결정한다. 재구성가능한 데이터 변형 유닛(906) 연산은 암호화/암호해독 라운드를 연산하도록 최적화되어 있다. 연산은, XOR, 우 쉬프트, 좌 쉬프트, 우로 회전, 좌로 회전, 비트-시리얼 대수, 치환, 순열, 신호 스왑(signal swap)를 포함하지만 이에 국한되어 있지 않다.

피연산자 메모리(908)는 도 8에서 신호 세트(806)의 서브셋인 신호(909)로부터 입력된 데이터를 수신한다. 데이터는 마이크로시퀀서(903)로부터의 신호(901)에 따라 메모리(908)로부터 페치된다. 페치된 데이터는 현재 구성 및 프로그램된 시퀀스에 따라 변형될 양방향 신호(907)을 거쳐 재구성가능한 데이터 변형 유닛(906)에 전달된다. 변형된 데이터는 양방향 신호(907)을 거쳐 피연산자 메모리(908)에 반환되거나 또는 도 8의 신호 세트(805)의 서브셋인 신호 세트(905)를 거쳐 재구성가능한 데이터 변형 유닛(906)으로부터 출력된다.

예시적인 실시예에서, 마이크로시퀀서(903)는 다수의 라운드(multiple rounds)를 수행하도록 프로그램되어 있어, 단일 커널(360)에 의해 실행될 수 있는 변형의 수를 증가시킨다. 다른 예시적인 실시예에서, 마이크로시퀀서(903)는 신호 세트(806)에 의해 제공되는 것보다 넓은 입력에 대해 다수의 사이클을 실행하도록 프로그램되어 있어, 암호화/암호해독 워드 폭을 효율적으로 증가시킨다. 선택적으로, 다수의 사이클을 수행하는 커널을 프로그래밍하는 동일한 효과 및 이점은, 소정의 워드 폭이 얻어질 때까지 인접하는 커널을 축약함으로써 실현될 수 있다. 축약은, 보다 많은 자원을 소비하지만, 동일한 수의 변형을 달성하는 시간을 감소시킨다.

다른 예시적인 실시예에서, 캐스케이드된 커널은 연속하는 라운드를 효과적으로 구현할 수 있어 전체적인 지연을 감소시킨다. 더우기, 캐스케이드된 커널은 암호-암호해독-암호와 같은 보다 복잡한 알고리즘을 구현하는데 사용될 수 있다.

도 10은 예시적인 보다 높은 성능의 암호/암호해독 커널(360)을 고시한다. 도 10에서, 커널(360)은 n-비트 폭 변형 슬라이스(1001)로 구성된 순수한 데이터경로 구조를 구비한다. 슬라이스(1001)는 도 8에서 신호(803)의 서브셋인 입력 및 제어 신호 세트(1003)를 거쳐 구성될 수 있다. 변형 슬라이스(1001)가 수행할 수 있는 연산의 세트는 XOR, 우 쉬프트, 좌 쉬프트, 우 회전, 좌 회전, 비트-시리얼 배수, 치환, 순열, 신호 스왑(signal swap) 및 프로그래머블 지연을 포함하지만 이에 국한되어 있지 않다. 일단 구성되면, 변형 슬라이스(1001)는 클럭 사이클 당 단일 연산을 수행한다. 한 변형 슬라이스(1001)의 출력은 입력 신호 세트(1002)를 거쳐 다음 변형 슬라이스(1001)에 입력된다. 커널 입력은 도 8에서 입력 신호 세트(806)의 서브셋인 신호 입력(1005)을 거쳐 인가된다. 커널 출력은 도 8에서 출력 신호 세트(805)의 서브셋인 신호 세트(1004)를 거쳐 존재한다.

도 11은 예시적인 통신 장치(1100)를 도시한다. 통신 장치(1100)는 프로그래머블 로직 장치(1102) 및 프로그래머블 보안 회로(1104)를 포함한다. 프로그래머블 로직 장치(1102)는 임의의 공지된 프로그래머블 로직 회로로서 구현될 수 잇다. 예를 들어, 작고, 중간 또는 큰 입자의 프로그래머블 로직 블럭이 프로그래머블 로직 장치(1102)에 구현될 수 있다. 프로그래머블 보안 회로(1104)는 휘발성, 비휘발성, 스태틱 또는 다이나믹 장치로서 구현될 수 있는 프로그래머블 로직 블럭이다.

예시적인 실시예에서, 프로그래머블 보안 회로(1104)는 두가지 모드로 동작한다. 제1 모드에서, 프로그래머블 보안 회로(1104)는 프로그래머블 로직 장치(1102)의 새로운 구성을 위한 인증을 제공한다. 제2 모드에서, 프로그래머블 보안 회로(1104)는 프로그래머블 로직 장치(1102)에 의해 수행될 수 있는 선택된 동작에 대한 인증을 제공한다.

보안 요청 및 리드-백(read-back) 라인(1106)은 보안 키 세트를 프로그래머블 보안 회로(1104)에 프로그램하는데 사용된다. 각각의 보안 키는 허용된 프로그래머블 로직 장치 구성 프로그래머블 로직 장치 동작을 명시한다.

프로그래머블 보안 회로(1104)가 프로그램된 후에, 보안 요청 및 리드-백 라인(1106)은 프로그래머블 로직 장치(1102)가 새로운 구성을 가질 수 있는 지의 여부를 결정하기 위해 프로그래머블 보안 회로(1104)를 질의하는데 사용될 수 있다. 프로그래머블 장치(1100)는 또한 새로운 구성을 프로그래머블 로직 장치(1102)에 제공하는 외부 구성 데이터 입력 라인(1108), 이와 같은 새로운 구성이 허용될 때 새로운 구성을 프로그래머블 로직 장치(1102)에 전달하거나 또는 요청된 동작에 대한 허가가 프로그래머블 보안 회로에 의해 허용될 때 프로그래머블 로직 장치(1102)에 인에이블 신호를 송신하는 허가 라인(1110), 및 프로그래머블 로직 장치(1102)로부터의 요청을 프로그래머블 보안 회로(1104)로 전달하여 동작을 수행하는 내부 동작 입력 라인(1112)를 구비한다.

도 12는 프로그래머블 보안 회로(1104)의 예시적인 실시예를 도시한다. 프로그래머블 보안 회로(1104)는 선형 피드백 쉬프트 레지스터(1202) 및 비교기 회로(1204)를 구비한다. 선형 피드백 쉬프트 레지스터(1202)는 리드-백 라인(1106)을 통해 보안 키를 저장한다. 보안 키가 선형 피드백 쉬프트 레지스터(1202)에 프로그램된 후에, 리드-백 라인(1106)은 보안 요청 라인으로 사용된다. 프로그래머블 로직 장치(1102)(도 11)는 동작을 수행하거나 재어 신호 또는 선정된 조건 세트에 응답해서 그 자신을 재구성하기 위해 요청할 수 있다. 입사하는 요청이 보안 요청 라인(1106)을 거쳐 프로그래머블 보안 회로(1202)에 도달하면, 비교기 회로(1204)는 선형 피드백 쉬프트 레지스터(1202) 내의 보안 키를 보안 요청 라인(1106)으로부터 입력된 요청과 비교한다. 만일 비교기 회로(1204)가 그 요청과, 선형 피드백 쉬프트 레지스터(1202)에 저장된 보안 키중의 하나 간의 일치를 발견하면, 프로그래머블 보안 회로(1404)는 요청된 동작 또는 재구성을 인증할 수 있다. 재구성 요청의 경우에, 제시된 구성이 외부 구성 데이터 입력 라인(1108)을 통해 다운로드될 수 있다. 다음에, 제시된 구성은 프로그래머블 로직 장치(1102)를 재구성하기 위해 허가 라인(1110)을 거쳐 프로그래머블 로직 장치(1102)에 전달된다. 만일 비교기 회로(1204)가 그 요청과, 선형 피드백 쉬프트 레지스터(1202)에 저장된 보안 키중의 하나 간의 일치를 발견하지 못하면, 프로그래머블 로직 장치(1102)는 새로운 구성을 수락하는 것이 금지될 것이다. 예시적인 실시예에서, 프로그래머블 로직 장치(1102)는 내부 동작 입력 라인(1112)을 통해 요청을 프로그래머블 보안 회로(1104)에 전달하여 수락가능한 동작을 증명한다. 만일 프로그래머블 보안 회로(1104)가 요청된 동작에 대한 일치하는 키를 포함하면, 이때 인에이블 신호가 허가 라인(1110)을 거쳐 전달되어, 프로그래머블 로직 장치(1102)를 인에이블시켜 요청된 동작을 수행하게 한다.

도 13은 본 발명의 실시예에 따른 예시적인 프로세스를 도시한다. 요청이 프로그래머블 보안 회로에 전달되어 임의의 동작을 수행하거나 또는 프로그래머블 로직 장치를 재구성한다. 프로그래머블 보안 회로는 요청을 수신한다(단계 1302). 프로그래머블 보안 회로는 이 요청을 이미 프로그램된 보안 키의 세트와 비교한다(단계 1304). 만일 요청된 동작/구성 간의 일치가 보안 키의 세트에서 발견되면(단계 1306), 프로그래머블 보안 회로는 요청을 인증한다(단계 1308). 만일 요청된 동작/구성 간의 일치가 보안 키의 세트에서 발견되지 않으면(단계 1306), 프로그래머블 보안 회로는 PLD가 새로운 구성을 수락하지 못하게 한다(단계 1310). 선택적으로, 프로그래머블 보안 회로는 허용불가능한 동작에 대한 동작에 대한 거절을 반환한다.

산업상 이용 가능성

기술분야의 숙련자는 본 발명이 서로 다른 데이터, 알고리즘, 루틴 또는 유틸리티가 실시간으로 로드될 수 있는 임의의 장치에서 성공적으로 이용될 수 있다는 것을 알 것이다. 예를 들어, 본 발명은 새로운 표준, 시스템 업그레이드, 및 시험 기간을 인에이블시키기 위한 것과 같은 지적소유권에 대한 라이센스를 제어하는데 유용하다. 따라서, 본 발명은 다중-모드 무선 텔레톤, 암호화 장치, 및 이미지 조작 장치와 같은 다중-모드 제품에 성공적으로 이용될 수 있다.

상기 예는, 다른 실시예, 변형 및 수정이 기술분야의 숙련자에게 명확한 본 발명의 임의의 예시적인 실시예를 도시한다. 따라서 본 발명은 상기 논의된 특정 실시예에 국한되지 않고, 첨부하는 특허청구의 범위에 의해 한정된다.

(57) 청구의 범위

청구항 1.

프로그래머블 재구성가능한(programmable reconfigurable) 보안 프로세서에 있어서,

재구성가능한 데이터 라우터; 및

상기 재구성가능한 데이터 라우터에 의해 상호접속된 프로그래머블 데이터 처리 커널의 세트

를 구비하여, 각각의 프로그래머블 데이터 처리 커널이 보안 알고리즘의 함수의 서브셋을 처리하도록 구성되어 있는 보안 프로세서.

청구항 2.

제1항에 있어서, 프로그래머블 데이터 처리 커널중의 적어도 하나는 수평으로 인접하는 프로그래머블 데이터 처리 커널에 상호접속되어 있는 보안 프로세서.

청구항 3.

제1항에 있어서, 프로그래머블 데이터 처리 커널중의 적어도 하나는 수직으로 인접하는 프로그래머블 데이터 처리 커널에 상호접속되어 있는 보안 프로세서.

청구항 4.

제1항에 있어서, 상기 프로그래머블 데이터 처리 커널은 프로그래머블 마이크로시퀀서, 재구성가능한 데이터 변형 유닛, 및 피연산자 메모리를 구비하는 보안 프로세서.

청구항 5.

제1항에 있어서, 상기 프로그래머블 데이터 처리 커널은 데이터경로 구조를 구비하는 보안 프로세서.

청구항 6.

제5항에 있어서, 상기 데이터경로 구조는 변형 슬라이스의 세트를 구비하는 보안 프로세서.

청구항 7.

디지털 로직 회로에 있어서,

프로그래머블 로직 장치; 및

인가된 구성(authorized configuration) 보안 키의 세트를 저장하는 프로그래머블 보안 회로

를 구비하되, 상기 프로그래머블 보안 회로는 상기 인가된 구성 보안 키를 들어오는 구성 요청과 비교하고, 상기 구성 요청에 응답해서 상기 프로그래머블 로직 장치에 대한 새로운 구성을 선택적으로 인에이블시키는 디지털 로직 회로.

청구항 8.

제7항에 있어서, 상기 프로그래머블 보안 회로는 선형 피드백 쉬프트 레지스터 및 비교기 회로를 구비하는 디지털 로직 회로.

청구항 9.

제8항에 있어서, 상기 선형 피드백 쉬프트 레지스터는 상기 인가된 구성 보안 키를 저장하도록 구성되어 있는 디지털 로직 회로.

청구항 10.

제8항에 있어서, 상기 비교기 회로는 상기 선형 피드백 쉬프트 레지스터에 저장된 상기 인가된 구성 보안 키에 대해 상기 들어오는 구성 요청을 비교하도록 구성되어 있는 디지털 로직 회로.

청구항 11.

디지털 로직 회로에 있어서,

프로그래머블 로직 장치; 및

인가된 동작(authorized operation) 보안 키의 세트를 저장하는 프로그래머블 보안 회로

를 구비하되, 상기 프로그래머블 보안 회로는 상기 인가된 동작 보안 키를 상기 프로그래머블 로직 장치로부터의 들어오는 동작 요청과 비교하교, 상기 동작요청에 응답해서 상기 프로그래머블 로직 장치 내의 동작을 선택적으로 인에이블시키는 디지털 로직 회로.

청구항 12.

제11항에 있어서, 상기 프로그래머블 보안 회로는 선형 피드백 쉬프트 레지스터 및 비교기 회로를 구비하는 디지털 로직 회로.

청구항 13.

제12항에 있어서, 상기 선형 피드백 쉬프트 레지스터는 상기 인가된 동작 보안 키를 저장하도록 구성되어 있는 디지털 로직 회로.

청구항 14.

제12항에 있어서, 상기 비교기 회로는 상기 선형 피드백 쉬프트 레지스터에 저장된 상기 인가된 동작 보안 키에 대해 상기 들어오는 동작 요청을 비교하도록 구성되어 있는 디지털 로직 회로.

청구항 15.

디지털 로직 회로에서의 요청을 처리하는 방법에 있어서,

요청을 수신하는 단계;

상기 요청을 프로그래머블 보안 회로 내의 프로그램된 보안 키의 세트와 비교하는 단계;

상기 요청과, 상기 프로그래머블 보안 키 회로의 상기 프로그램된 보안 키의 세트 간에 일치가 발견되면 상기 요청에 대해 허가를 발행하는 단계; 및

상기 요청과, 상기 프로그래머블 보안 회로 내의 상기 프로그램된 보안 키의 세트 간에 일치가 발견되지 않으면 상기 요청에 대해 거절을 발행하는 단계

를 포함하는 방법.

청구항 16.

제15항에 있어서, 상기 수신은 구성 요청을 수신하는 방법.

청구항 17.

제15항에 있어서, 상기 프로그램된 보안 키의 세트는 인가된 구성 보안 키를 포함하는 방법.

청구항 18.

제15항에 있어서, 상기 수신은 동작 요청을 포함하는 방법.

청구항 19.

제15항에 있어서, 상기 프로그램된 보안 키의 세트는 인가된 동작 보안 키를 포함하는 방법.

청구항 20.

보안 프로세서를 구성하여 네트워크에 걸쳐 수신된 보안 알고리즘을 처리하는 방법에 있어서,

네트워크에 걸쳐 해더부를 포함하는 보안 알고리즘을 수신하는 단계;

상기 헤더부를 파싱하여 자격 및 규정 정보(regulatory information)를 검색하는 단계;

상기 자격 및 규정 정보에 적어도 부분적으로 기초하여 파라메타의 세트를 발생하는 단계;

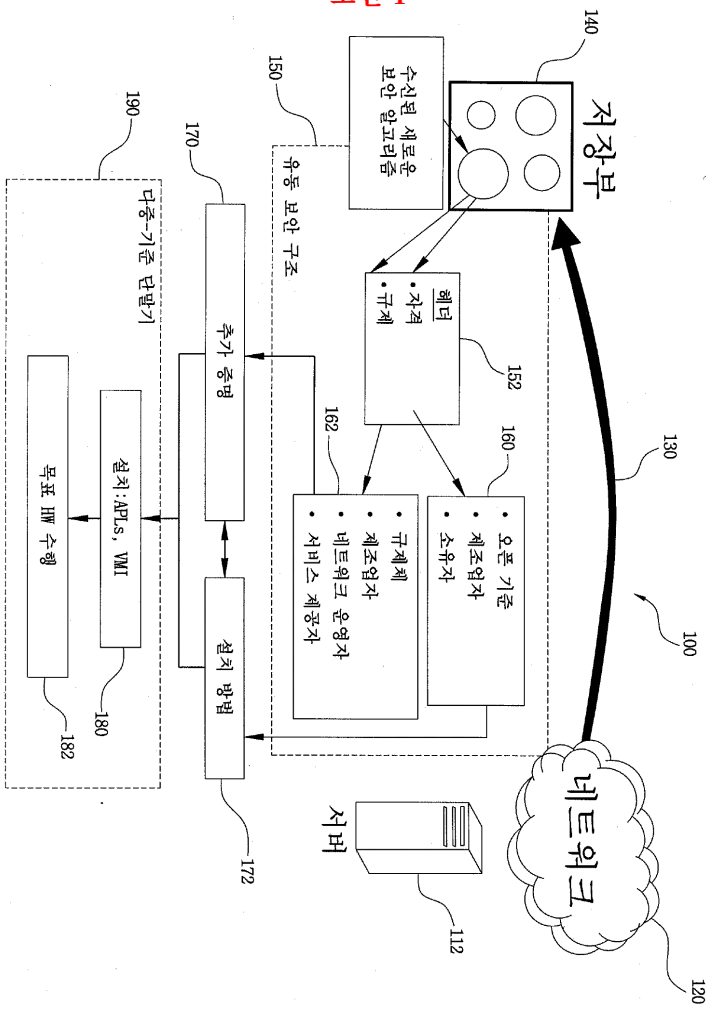
상기 보안 알고리즘을 설치하는 단계; 및

상기 파라메타의 세트에 따라 보안 프로세서를 구성하는 단계

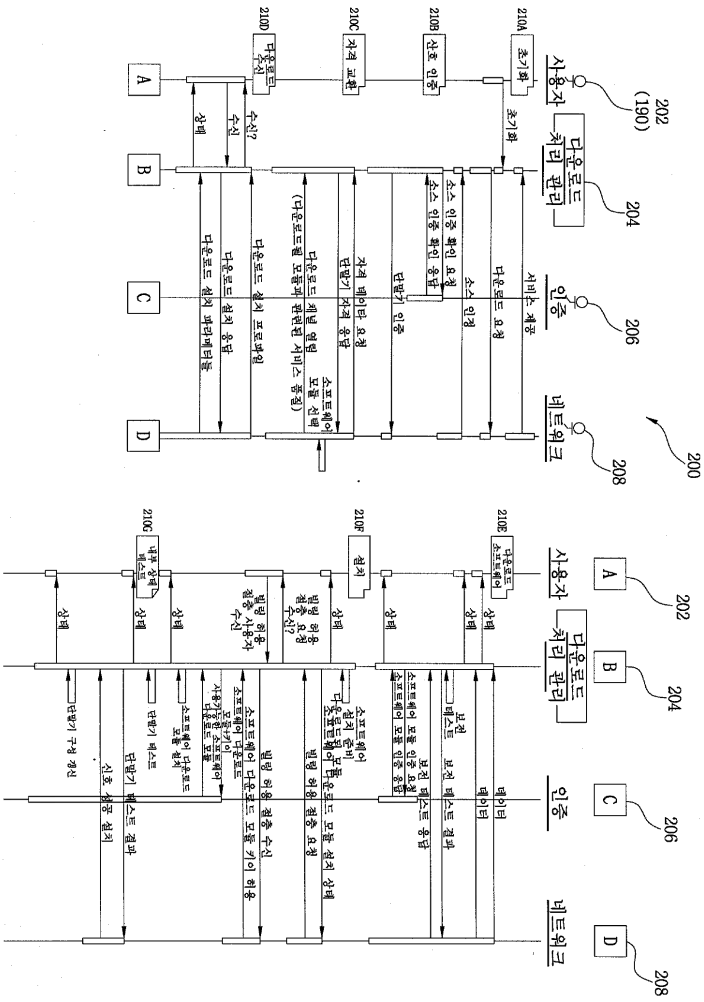
를 포함하는 방법.

도면

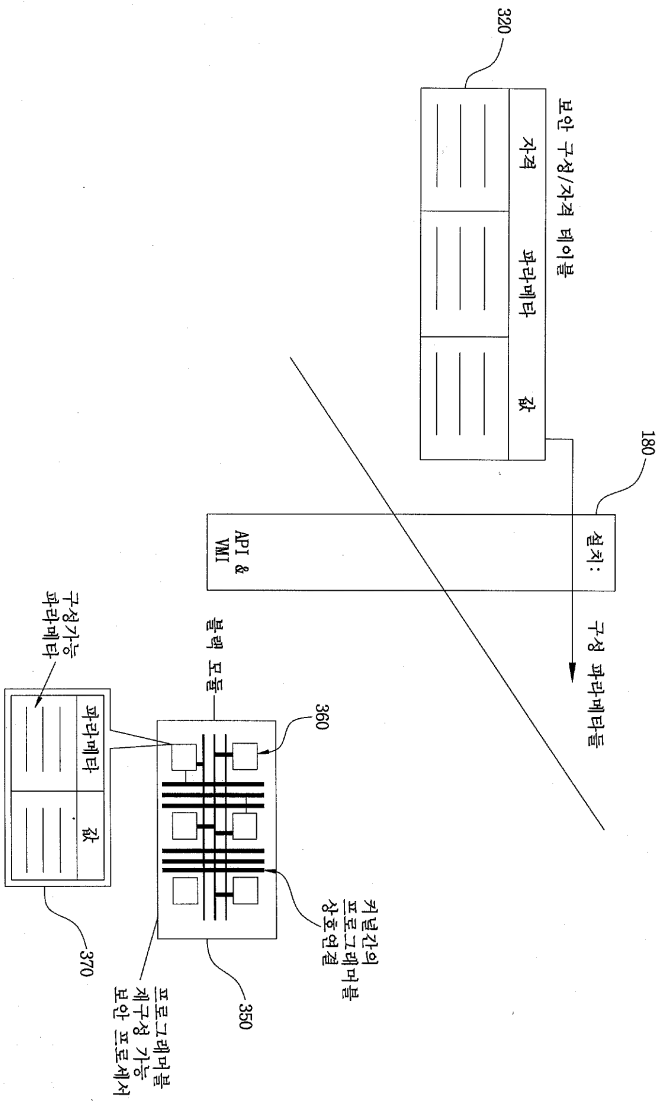
도면 1


140
저장부
수신된 새로운 보안 알고리즘
150
유동 보안 구조
헤더
• 자격
• 규제
152
160
• 오픈 기준
• 제조업자
• 소유자
162
• 규제체
• 제조업자
• 네트워크 운영자
• 서비스 제공자
130
100
네트워크
120
서버
112
190
다중-기준 단말기
170
추가 증명
설치 방법
172
설치: APLs, VMI
목표 HW 수행
180
182

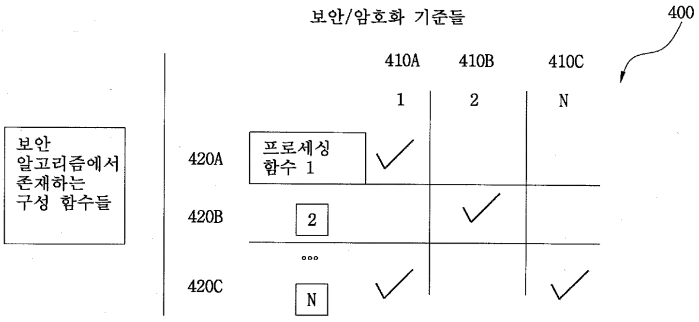
도면 2


사용자
(190)
202
다운로드 처리 관리
204
인증
206
네트워크
208
200
A
B
C
D
초기화
산호 인증
차례 교환
다운로드 수신
상태
수신?
서비스 제공
다운로드 요청
소스 인증 확인 요청
소스 인증 확인 응답
다운로드 설치 프로파일
다운로드 설치 응답
다운로드 설치 파라메터들
(다운로드될 모듈과 관련된 서비스 품질)
소프트웨어 모듈 선택
다운로드 케넘 얼림
단말기 인증
단말기 차례 요청
단말기 차례 응답
네트워크 상태
설치
소프트웨어 모듈 인증 요청
소프트웨어 모듈 인증 응답
보관 테스트 결과
테스트 보관
데이터
데이터
소프트웨어 다운로드 모듈 설치 상태
얼림 허용 철증 요청
얼림 허용 철증 수신
소프트웨어 다운로드 모듈 키이 허용
소프트웨어 다운로드 모듈 설치
소프트웨어 다운로드 모듈 설치 결과
단말기 구성 갱신
단말기 테스트
신호 철증 설치

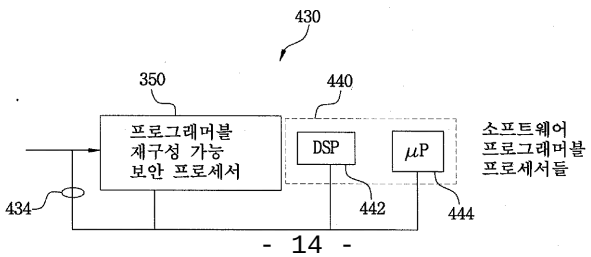
도면 3



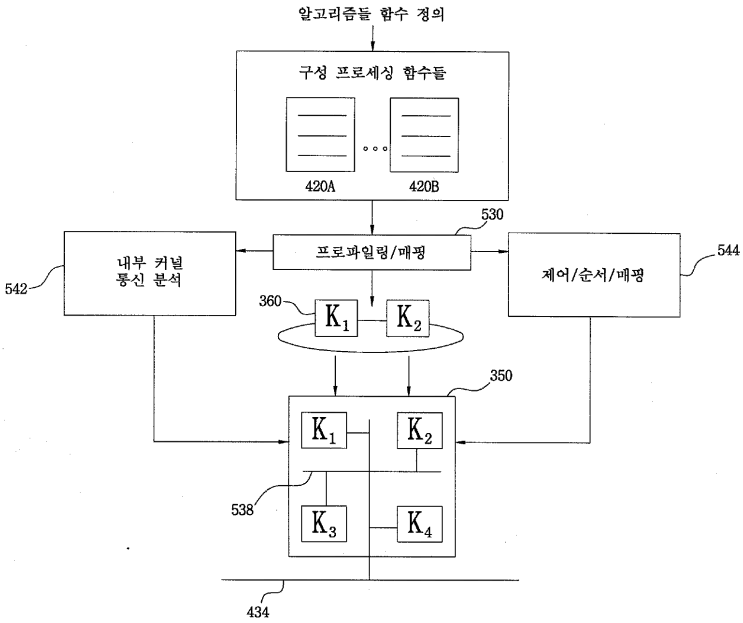
도면 4a



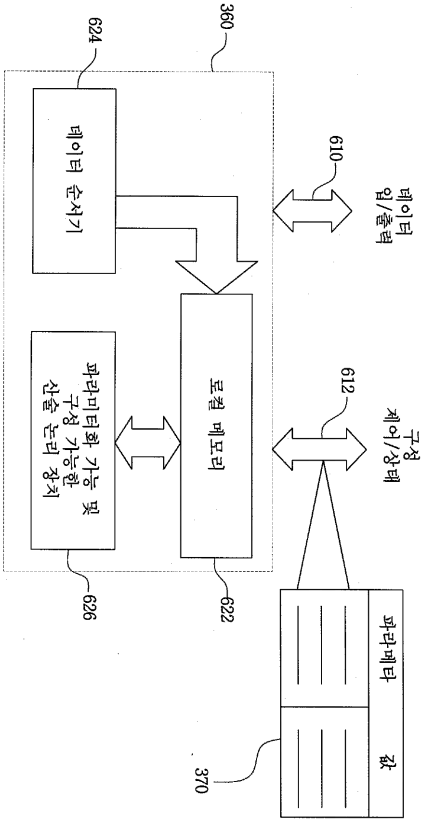
도면 4b



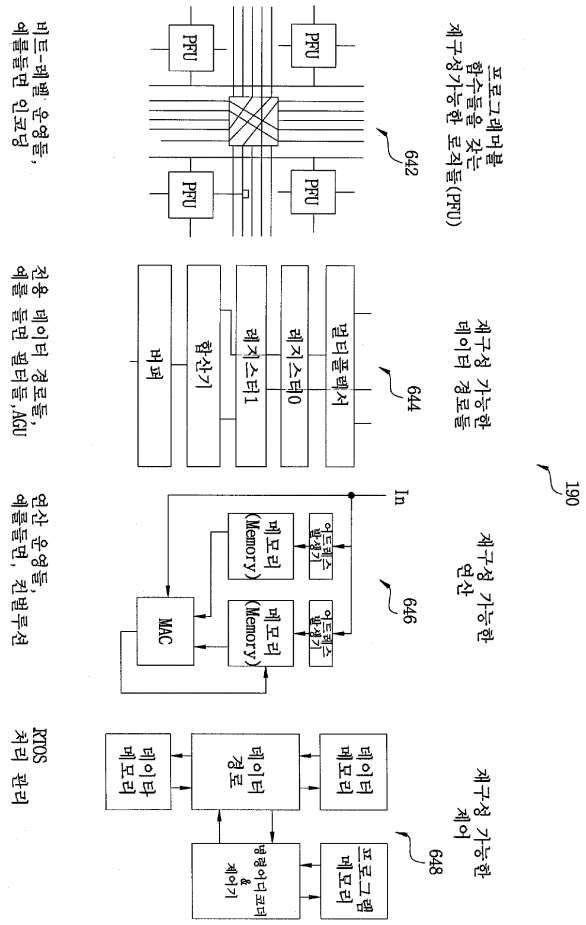
도면 5


알고리즘들 함수 정의
구성 프로세싱 함수들
420A
420B
530
내부 커널
통신 분석
542
프로파일링/매핑
제어/순서/매핑
544
360
K1
K2
350
K1
K2
538
K3
K4
434

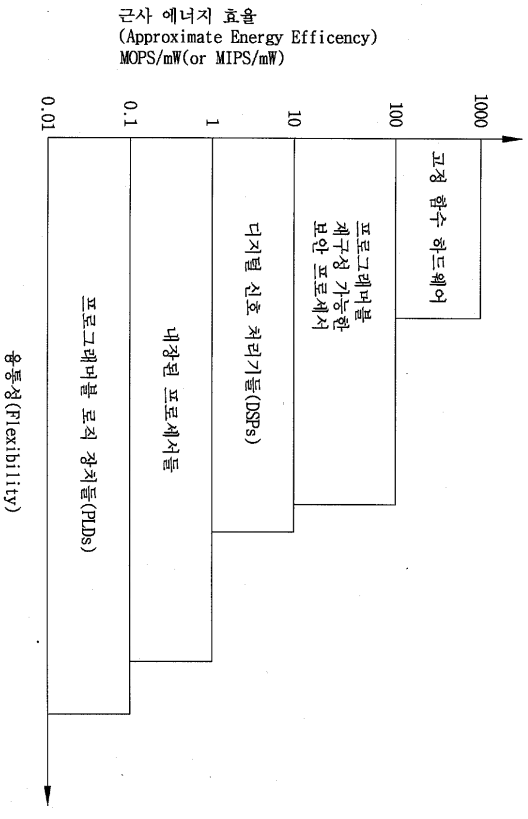
도면 6a


624
360
데이터 순서기
610
데이터
입/출력
파라미터화 가능 및
구성 가능한
산술 논리 장치
로컬 메모리
612
구성
제어/상태
626
622
파라메타
값
370

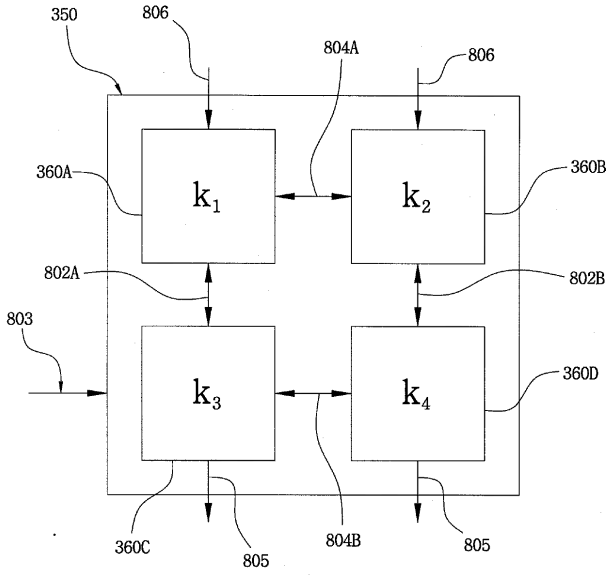
도면 6b


190
642
644
646
648
In
PFU
PFU
PFU
PFU
멀티플렉서
레지스터0
레지스터1
합산기
버퍼
메모리 (Memory)
메모리 (Memory)
MAC
데이타 메모리
데이터 경로
프로그램 메모리
병렬어드레스 & 제어기
프로그래머블 함수들을 갖는 재구성가능한 로직들(PFU)
재구성 가능한 데이터 경로들
재구성 가능한 연산
재구성 가능한 제어
비트-레벨 운영들, 예를들면 인코딩
전용 데이터 경로들, 예를 들면 필터들,AGU
연산 운영들, 예를들면, 컨벌루션
RTOS 처리 관리

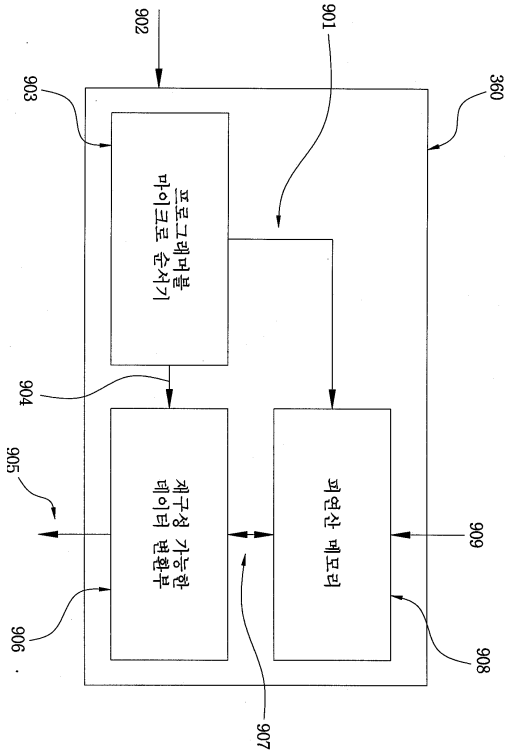
도면 7


근사 에너지 효율
(Approximate Energy Efficency)
MOPS/mW(or MIPS/mW)
1000
100
10
1
0.1
0.01
고정 함수 하드웨어
프로그래머블 재구성 가능한 보안 프로세서
디지털 신호 처리기들(DSPs)
내장된 프로세서들
프로그래머블 로직 장치들(PLDs)
융통성(Flexibility)

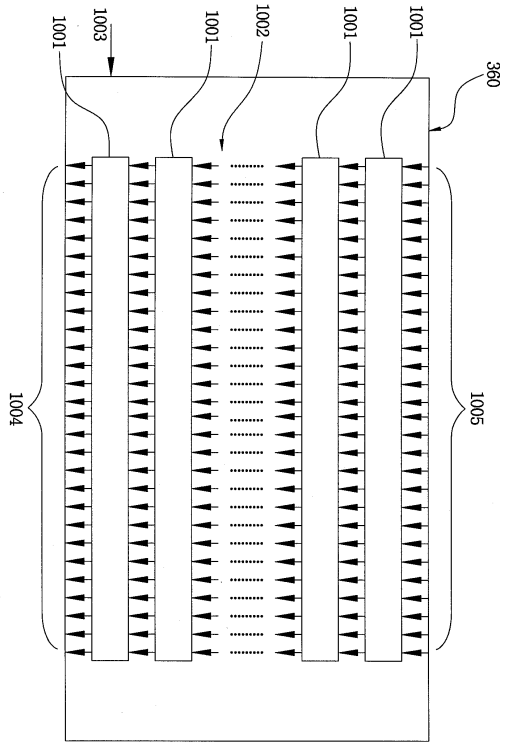
도면 8


350
806
804A
806
360A
k_1
k_2
360B
802A
802B
803
k_3
k_4
360D
360C
805
804B
805

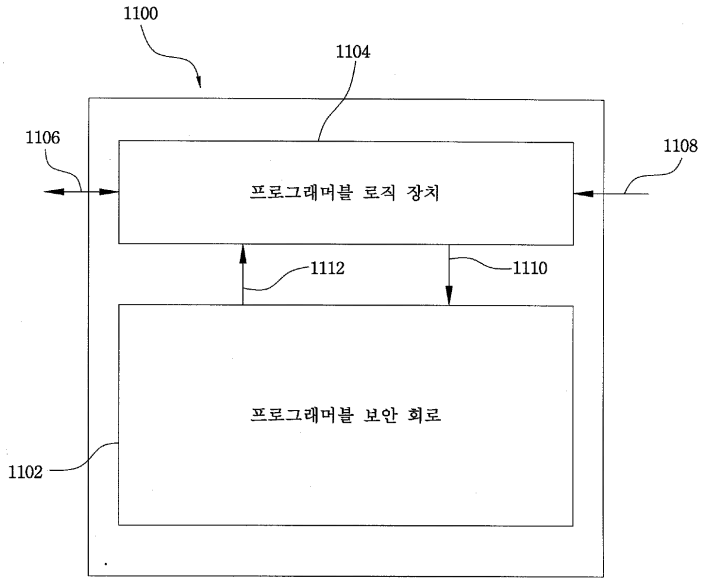
도면 9


902
901
903
360
프로그래머블 마이크로 순서기
904
905
재구성 기능형 데이터 변환부
피연산 메모리
909
906
908
907

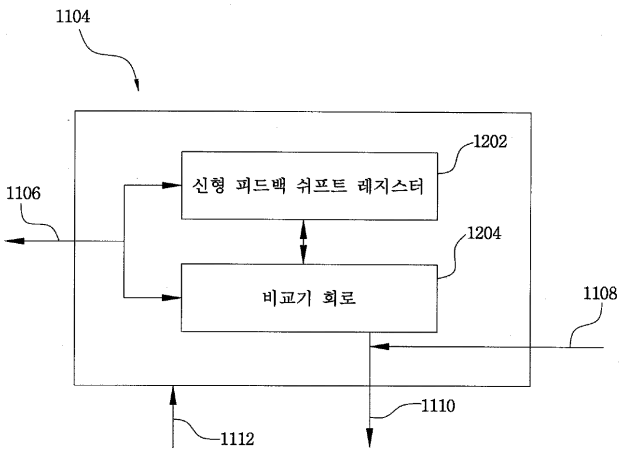
도면 10


1001
1003
1001
1002
1001
1001
360
1004
1005

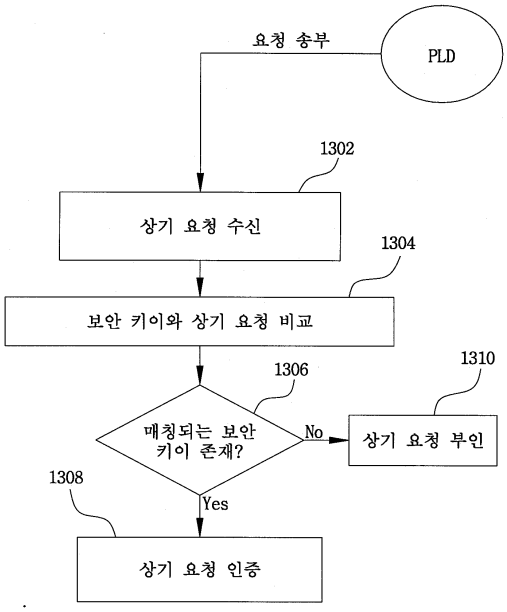
도면 11


1100
1104
1106
1108
프로그래머블 로직 장치
1112
1110
프로그래머블 보안 회로
1102

도면 12


1104
1202
신형 피드백 쉬프트 레지스터
1106
1204
비교기 회로
1108
1110
1112

도면 13


요청 송부
PLD
1302
상기 요청 수신
1304
보안 키이와 상기 요청 비교
1306
매칭되는 보안 키이 존재?
No
1310
상기 요청 부인
1308
Yes
상기 요청 인증