(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2008년02월01일
(11) 등록번호 10-0800468
(24) 등록일자 2008년01월28일

(51) Int. Cl.
H04L 9/14 (2006.01)
(21) 출원번호 10-2004-0005647
(22) 출원일자 2004년01월29일
심사청구일자 2004년01월29일
(65) 공개번호 10-2005-0078271
(43) 공개일자 2005년08월05일
(56) 선행기술조사문헌
KR1020020087331 A
US20030133568 A1
논문
1020040005647 - 594144
전체 청구항 수 : 총 24 항

(73) 특허권자
삼성전자주식회사
경기도 수원시 영통구 매탄동 416
(72) 발명자
안경문
서울특별시관악구봉천5동1712
번지관악드림타운119-2201
노미정
경기도용인시수지읍상현리성원1차아파트101-804
(74) 대리인
리앤목특허법인, 이해영

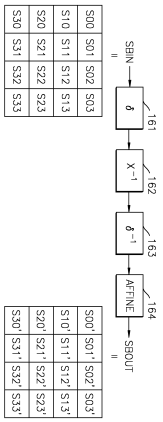
심사관 : 이준석

(54) 저전력 고속 동작을 위한 하드웨어 암호화/복호화 장치 및그 방법

(57) 요 약

저전력 고속 동작을 위한 하드웨어 암호화/복호화 장치 및 그 방법이 개시된다. 상기 하드웨어 암호화/복호화 장치는, 라운드 연산부에서 각 라운드 연산에 해당하는 키들을 입력받아, 입력 데이터를 암호문으로 변환한다. 상기 하드웨어 암호화/복호화 장치의 S-BOX 연산 또는 역 S-BOX 연산은, 갈로아 필드 $GF(2^8)$ 상의 원소를 갈로아 필드 $GF(((2^2)^2)^2)$ 상의 원소로 변환한 뒤 합성 필드(Composite field)를 이용하여 원소의 곱셈의 역원을 계산하고, 상기 계산 결과를 이용하여 입력받는 벡터를 다른 벡터로 치환한다.

대표도 - 도5



특허청구의 범위

청구항 1

각 라운드에 해당하는 N개의 키들을 입력받아, 제1 라운드에서 상기 키들 중 제1 키를 이용하여 입력 데이터를 암호문으로 변환하고, 나머지 N-1 라운드 각각에서 순차적으로 상기 키들 중 제2 키 내지 제N 키를 이용하여 이전 라운드의 변환 결과를 다른 암호문으로 변환하는 라운드 연산부; 및

입력키를 이용하여 상기 제1 키 내지 상기 제N 키 각각을 생성하는 키 스케쥴러를 구비하고, 상기 라운드 각각은,

갈로아 필드 $GF(2^8)$ 상의 원소를 갈로아 필드 $GF(((2^2)^2)^2)$ 상의 원소로 변환한 뒤 합성 필드(Composite field)를 이용하여 원소의 곱셈의 역원을 계산하고, 상기 계산 결과를 이용하여 입력받는 벡터를 다른 벡터로 치환하는 S-BOX를 구비하며,

상기 S-BOX는,

입력받는 벡터의 각 원소를 이루는 갈로아 필드 $GF(2^8)$ 상의 원소를 갈로아 필드 $GF(((2^2)^2)^2)$ 상의 원소로 변환하는 델타 변환부;

갈로아 필드 $GF((2^2)^2)$ 상에서의 역원 계산을 통하여 갈로아 필드 $GF(((2^2)^2)^2)$ 상의 원소의 역원을 계산하여 출력하는 역원 계산부;

상기 갈로아 필드 $GF(((2^2)^2)^2)$ 상의 원소의 역원을 갈로아 필드 $GF(2^8)$ 상의 원소로 변환하는 역 델타 변환부; 및

아핀 함수에 따라 상기 변환된 갈로아 필드 $GF(2^8)$ 상의 원소를 아핀 변환하는 아핀 변환부를 포함하고,

상기 역원 계산부는, 상기 갈로아 필드 $GF(((2^2)^2)^2)$ 상의 원소를 이루는 8비트 디지털 데이터를 하위 4비트와 상위 4비트 데이터로 분류하여, 상기 분류된 4비트 데이터들 각각에 대하여, 합산과 승산으로 단순화된 연산을 통해 생성된 갈로아 필드 $GF((2^2)^2)$상의 원소를 입력받아 상기 갈로아 필드 $GF((2^2)^2)$ 상에서 역원을 계산하는 제1 역원 계산기를 포함하고,

상기 제1 역원 계산기는, 상기 갈로아 필드 $GF((2^2)^2)$ 상의 원소를 이루는 4비트 디지털 데이터를 하위 2비트와 상위 2비트 데이터로 분류하여, 상기 분류된 2비트 데이터들 각각에 대하여, 합산과 승산으로 단순화된 연산을 통해 생성된 갈로아 필드 $GF(2^2)$ 상의 원소를 입력받아 갈로아 필드 $GF(2^2)$ 상에서 역원을 계산하는 제2 역원 계산기를 포함하고,

상기 제2 역원 계산기는, 입력의 자승을 계산하여 역원으로서 출력하는 것을 특징으로 하는 하드웨어 암호화/복호화 장치.

청구항 2

제 1항에 있어서, 상기 하드웨어 암호화/복호화 장치는,

전송할 데이터와 상기 입력키를 합산하여, 그 합산 결과를 상기 입력 데이터로서 출력하는 합산기를 더 구비하는 것을 특징으로 하는 하드웨어 암호화/복호화 장치.

청구항 3

제 1항에 있어서, 상기 N은,

10인 것을 특징으로 하는 하드웨어 암호화/복호화 장치.

청구항 4

제 1항에 있어서, 상기 N은,

12인 것을 특징으로 하는 하드웨어 암호화/복호화 장치.

청구항 5

제 1항에 있어서, 상기 N은,

14인 것을 특징으로 하는 하드웨어 암호화/복호화 장치.

청구항 6

제 1항에 있어서, 상기 제1 라운드 내지 상기 제N-1 라운드 각각은,

상기 S-BOX를 이용하는 Sub_Byte 회로의 출력 신호를 입력 벡터로 받아, 로우 단위로 쉬프트 처리하는 함수에 따라 상기 입력 벡터를 로우 단위로 쉬프트 처리하여 출력하는 Shift_Row 회로;

컬럼 단위로 치환 처리하는 함수에 따라 상기 Shift_Row 회로의 출력 벡터를 컬럼 단위로 치환 처리하여 출력하는 Mix_Column 회로; 및

상기 Mix_Column 회로의 출력 벡터와 상기 키들 중 해당 라운드 키를 합산하여 출력하는 합산기를 더 구비하고,

상기 제N 라운드는,

상기 Sub_Byte 회로의 출력 신호를 입력 벡터로 받아, 로우 단위로 쉬프트 처리하는 함수에 따라 상기 입력 벡터를 로우 단위로 쉬프트 처리하여 출력하는 Shift_Row 회로; 및

상기 Shift_Row 회로의 출력 벡터와 상기 키들 중 해당 라운드 키를 합산하여 출력하는 합산기를 더 구비하는 것을 특징으로 하는 하드웨어 암호화/복호화 장치.

청구항 7

제 1항에 있어서, 상기 S-BOX는,

입력받는 벡터의 각 원소를 이루는 갈로아 필드 $GF(2^8)$ 상의 원소를 갈로아 필드 $GF(((2^2)^2)^2)$ 상의 원소로 변환하는 델타 변환부;

상기 갈로아 필드 $GF(((2^2)^2)^2)$ 상의 원소의 역원을 계산하여 출력하는 역원 계산부;

상기 갈로아 필드 $GF(((2^2)^2)^2)$ 상의 원소의 역원을 갈로아 필드 $GF(2^8)$ 상의 원소로 변환하는 역 델타 변환부; 및

아핀 함수에 따라 상기 변환된 갈로아 필드 $GF(2^8)$ 상의 원소를 아핀 변환하는 아핀 변환부를 구비하는 것을 특징으로 하는 하드웨어 암호화/복호화 장치.

청구항 8

제 7항에 있어서, 상기 역원 계산부는,

상기 갈로아 필드 $GF(((2^2)^2)^2)$ 상의 원소를 이루는 8비트 디지털 데이터의 하위 4비트와 상위 4비트 데이터를 제1 합산하는 제1 합산기;

갈로아 필드 $GF((2^2)^2)$ 상에서 상기 제1 합산 결과에 상기 하위 4비트 데이터를 제1 승산하는 제1 승산기;

상기 상위 4비트 데이터를 제1 자승하는 제1 자승기;

상기 제1 자승 결과에 제1 계수를 승산하는 제1 계수 승산기;

상기 제1 승산 결과와 상기 제1 자승 결과를 제2 합산하는 제2 합산기;

상기 갈로아 필드 $GF((2^2)^2)$ 상에서 상기 제2 합산 결과의 역원을 계산하는 제1 역원 계산기;

갈로아 필드 $GF((2^2)^2)$ 상에서 상기 제2 합산 결과의 역원에 상기 제1 합산 결과를 제2 승산하여, 상기 제2 승산

결과를 상기 하위 4비트 데이터의 역원으로서 출력하는 제2 승산기; 및

갈로아 필드 GF($(2^2)^2$) 상에서 상기 제2 합산 결과의 역원에 상기 상위 4비트 데이터를 제3 승산하여, 상기 제3 승산 결과를 상기 상위 4비트 데이터의 역원으로서 출력하는 제3 승산기를 구비하는 것을 특징으로 하는 하드웨어 암호화/복호화 장치.

청구항 9

제 8항에 있어서, 상기 제1 역원 계산기는,

상기 제2 합산 결과를 이루는 4비트 디지털 데이터의 하위 2비트와 상위 2비트 데이터를 제3 합산하는 제3 합산기;

갈로아 필드 GF(2^2) 상에서 상기 제3 합산 결과에 상기 하위 2비트 데이터를 제4 승산하는 제4 승산기;

상기 상위 2비트 데이터를 제2 자승하는 제2 자승기;

상기 제2 자승 결과에 제2 계수를 승산하는 제2 계수 승산기;

상기 제4 승산 결과와 상기 제2 계수 승산 결과를 제4 합산하는 제4 합산기;

상기 제4 합산 결과의 자승을 계산하여 상기 제4 합산 결과의 역원으로서 출력하는 제2 역원 계산기;

갈로아 필드 GF(2^2) 상에서 상기 제4 합산 결과의 역원에 상기 제3 합산 결과를 제5 승산하여, 상기 제5 승산 결과를 상기 하위 2비트 데이터의 역원으로서 출력하는 제5 승산기; 및

상기 갈로아 필드 GF(2^2) 상에서 상기 제4 합산 결과의 역원에 상기 상위 2비트 데이터를 제6 승산하여, 상기 제6 승산 결과를 상기 상위 2비트 데이터의 역원으로서 출력하는 제6 승산기를 구비하는 것을 특징으로 하는 하드웨어 암호화/복호화 장치.

청구항 10

제 8항에 있어서, 상기 제1 승산기 내지 제3 승산기 각각은,

2개의 4비트 디지털 데이터들을 제1 데이터 및 제2 데이터로서 입력받아, 갈로아 필드 GF($(2^2)^2$) 상에서 상기 4비트 데이터의 승산값을 계산하고,

상기 제2 데이터의 하위 2비트와 상위 2비트 데이터를 제5 합산하는 제5 합산기;

상기 제1 데이터의 하위 2비트와 상위 2비트 데이터를 제6 합산하는 제6 합산기;

갈로아 필드 GF(2^2) 상에서 상기 제1 데이터 및 상기 제2 데이터의 하위 2비트 데이터를 제7 승산하는 제7 승산기;

상기 갈로아 필드 GF(2^2) 상에서 상기 제1 데이터 및 상기 제2 데이터의 상위 2비트 데이터를 제8 승산하는 제8 승산기;

상기 갈로아 필드 GF(2^2) 상에서 상기 제5 합산 결과에 상기 제6 합산 결과를 제9 승산하는 제9 승산기;

상기 제9 승산 결과와 상기 제7 승산 결과를 제7 합산하여, 상기 제7 합산 결과를 상기 4비트 데이터의 승산값의 상위 2비트 데이터로서 출력하는 제7 합산기;

상기 제8 승산 결과에 제2 계수를 승산하는 제2 계수 승산기; 및

상기 제7 승산 결과와 제2 계수 승산 결과를 제8 합산하여, 상기 제8 합산 결과를 상기 4비트 데이터의 승산값의 하위 2비트 데이터로서 출력하는 제8 합산기를 구비하는 것을 특징으로 하는 하드웨어 암호화/복호화 장치.

청구항 11

제 9항에 있어서, 상기 제4 승산기 내지 제6 승산기 각각은,

2개의 2비트 디지털 데이터들을 제1 데이터 및 제2 데이터로서 입력받아, 갈로아 필드 GF(2^2) 상에서 상기 2비트 데이터의 승산값을 계산하고,

상기 제1 데이터 및 상기 제2 데이터의 상위 비트 데이터를 제1 논리곱 연산하는 제1 논리곱 로직;

상기 제1 데이터의 하위 비트와 상기 제2 데이터의 상위 비트를 제2 논리곱 연산하는 제2 논리곱 로직;

상기 제1 데이터의 상위 비트와 상기 제2 데이터의 하위 비트를 제3 논리곱 연산하는 제3 논리곱 로직;

상기 제1 데이터 및 상기 제2 데이터의 하위 비트 데이터를 제4 논리곱 연산하는 제4 논리곱 로직;

상기 제1 논리곱 및 상기 제2 논리곱 연산 결과들을 제1 배타적 논리합 연산하는 제1 배타적 논리합 로직;

상기 제1 배타적 논리합 연산 결과와 상기 제3 논리곱 연산 결과를 제2 배타적 논리합 연산하여, 상기 제2 배타적 논리합 연산 결과를 상기 2비트 데이터의 승산값의 상위 비트 데이터로서 출력하는 제2 배타적 논리합 로직; 및

상기 제1 논리곱 및 상기 제4 논리곱 연산 결과들을 제3 배타적 논리합 연산하여, 상기 제3 배타적 논리합 연산 결과를 상기 2비트 데이터의 승산값의 하위 비트 데이터로서 출력하는 제3 배타적 논리합 로직을 구비하는 것을 특징으로 하는 하드웨어 암호화/복호화 장치.

청구항 12

제 10항에 있어서, 상기 제7 승산기 내지 제9 승산기 각각은,

2개의 2비트 디지털 데이터들을 제3 데이터 및 제4 데이터로서 입력받아, 갈로아 필드 GF(2^2) 상에서 상기 2비트 데이터의 승산값을 계산하고,

상기 제3 데이터 및 상기 제4 데이터의 상위 비트 데이터를 제1 논리곱 연산하는 제1 논리곱 로직;

상기 제3 데이터의 하위 비트와 상기 제4 데이터의 상위 비트를 제2 논리곱 연산하는 제2 논리곱 로직;

상기 제3 데이터의 상위 비트와 상기 제4 데이터의 하위 비트를 제3 논리곱 연산하는 제3 논리곱 로직;

상기 제3 데이터 및 상기 제4 데이터의 하위 비트 데이터를 제4 논리곱 연산하는 제4 논리곱 로직;

상기 제1 논리곱 및 상기 제2 논리곱 연산 결과들을 제1 배타적 논리합 연산하는 제1 배타적 논리합 로직;

상기 제1 배타적 논리합 연산 결과와 상기 제3 논리곱 연산 결과를 제2 배타적 논리합 연산하여, 상기 제2 배타적 논리합 연산 결과를 상기 2비트 데이터의 승산값의 상위 비트 데이터로서 출력하는 제2 배타적 논리합 로직; 및

상기 제1 논리곱 및 상기 제4 논리곱 연산 결과들을 제3 배타적 논리합 연산하여, 상기 제3 배타적 논리합 연산 결과를 상기 2비트 데이터의 승산값의 하위 비트 데이터로서 출력하는 제3 배타적 논리합 로직을 구비하는 것을 특징으로 하는 하드웨어 암호화/복호화 장치.

청구항 13

제 2항에 있어서, 상기 키 스케쥴러는,

상기 입력키를 이용하여 상기 제1 라운드에서 사용될 상기 제1 키를 생성하고, 상기 나머지 N-1 라운드들 각각에서 사용될 상기 제2 키 내지 상기 제N 키는 이전 라운드에서 사용되는 키가 저장되는 레지스터 값을 이용하여 순차적으로 발생시키며, 상기 합산기에 상기 입력키의 제공과 상기 제1 키의 발생은 소정 클럭의 한 싸이클에 이루어지는 것을 특징으로 하는 하드웨어 암호화/복호화 장치.

청구항 14

N개의 라운드들에 대응하는 해당 N개의 키들을 입력받는 단계;

상기 라운드들 중 제1 라운드에서 상기 키들 중 제1 키를 이용하여 입력 데이터를 암호문으로 변환하는 단계;

나머지 N-1 라운드들 각각에서 순차적으로 상기 키들 중 제2 키 내지 제N 키를 이용하여 이전 라운드의 변환 결과를 다른 암호문으로 변환하는 단계; 및

입력키를 이용하여 상기 제1 키 내지 상기 제N 키 각각을 생성하는 단계를 구비하고, 상기 라운드들 각각의 암호문으로 변환 단계는,

S-BOX 연산에서, 갈로아 필드 GF(2^8) 상의 원소를 갈로아 필드 GF($(((2^2)^2)^2$) 상의 원소로 변환한 뒤 합성 필드(Composite)를 이용하여 원소의 곱셈의 역원을 계산하고, 입력받는 벡터를 상기 계산 결과를 이용하여 다른 벡터로 치환하는 단계를 구비하며,

상기 치환하는 단계는,

입력받는 벡터의 각 원소를 이루는 갈로아 필드 GF(2^8) 상의 원소를 갈로아 필드 GF($(((2^2)^2)^2$) 상의 원소로 변환하는 단계;

상기 갈로아 필드 GF($(((2^2)^2)^2$) 상의 원소의 역원을 계산하여 출력하는 단계;

상기 갈로아 필드 GF($(((2^2)^2)^2$) 상의 원소의 역원을 갈로아 필드 GF(2^8) 상의 원소로 변환하는 단계; 및

아핀 함수에 따라 상기 변환된 갈로아 필드 GF(2^8) 상의 원소를 아핀 변환하는 단계를 포함하고,

상기 갈로아 필드 GF($(((2^2)^2)^2$) 상의 원소의 역원 계산은, 상기 갈로아 필드 GF($(((2^2)^2)^2$) 상의 원소를 이루는 8비트 디지털 데이터를 하위 4비트와 상위 4비트 데이터로 분류하여, 상기 분류된 4비트 데이터들 각각에 대하여, 합산과 승산으로 단순화된 연산을 이용하여 갈로아 필드 GF($(2^2)^2$) 상에서 역원을 계산하고,

상기 갈로아 필드 GF($(2^2)^2$) 상의 원소의 역원 계산은,

상기 갈로아 필드 GF($(2^2)^2$) 상의 원소를 이루는 4비트 디지털 데이터를 하위 2비트와 상위 2비트 데이터로 분류하여, 상기 분류된 2비트 데이터들 각각에 대하여, 합산과 승산으로 단순화된 연산을 이용하여 갈로아 필드 GF(2^2) 상에서 역원을 계산하는 것을 특징으로 하는 하드웨어 암호화/복호화 방법.

청구항 15

제 14항에 있어서, 상기 하드웨어 암호화/복호화 방법은,

전송할 데이터와 상기 입력키를 합산하여, 그 합산 결과를 상기 입력 데이터로서 출력하는 단계를 더 구비하는 것을 특징으로 하는 하드웨어 암호화/복호화 방법.

청구항 16

제 14항에 있어서, 상기 N은,

10인 것을 특징으로 하는 하드웨어 암호화/복호화 방법.

청구항 17

제 14항에 있어서, 상기 제1 라운드 내지 상기 제N-1 라운드 각각에서 암호문으로 변환 단계는,

입력되는 신호를 입력 벡터로 받아, 상기 S-BOX 연산을 수행하여 그 수행 결과를 출력하는 단계;

로우 단위로 쉬프트 처리하는 함수에 따라 상기 S-BOX 연산 결과를 로우 단위로 쉬프트 처리하여 출력하는 단계;

컬럼 단위로 치환 처리하는 함수에 따라 상기 로우 단위로 쉬프트 처리된 벡터를 컬럼 단위로 치환 처리하여 출력하는 단계; 및

상기 컬럼 단위로 치환 처리된 벡터와 상기 키들 중 해당 라운드 키를 합산하여 출력하는 단계를 구비하고,

상기 제N 라운드에서 암호문으로 변환 단계는,

입력되는 신호를 입력 벡터로 받아, 상기 S-BOX 연산을 수행하여 그 수행 결과를 출력하는 단계;

로우 단위로 쉬프트 처리하는 함수에 따라 상기 S-BOX 연산 결과를 로우 단위로 쉬프트 처리하여 출력하는

단계; 및

상기 로우 단위로 쉬프트 처리된 벡터와 상기 키들 중 해당 라운드 키를 합산하여 출력하는 단계를 구비하는 것을 특징으로 하는 하드웨어 암호화/복호화 방법.

청구항 18

제 14항에 있어서, 상기 치환 단계는,

입력받는 벡터의 각 원소를 이루는 갈로아 필드 GF(2^8) 상의 원소를 갈로아 필드 GF(((2^2)^2)^2) 상의 원소로 변환하는 단계;

상기 갈로아 필드 GF(((2^2)^2)^2) 상의 원소의 역원을 계산하여 출력하는 단계;

상기 갈로아 필드 GF(((2^2)^2)^2) 상의 원소의 역원을 갈로아 필드 GF(2^8) 상의 원소로 변환하는 단계; 및

아핀 함수에 따라 상기 변환된 갈로아 필드 GF(2^8) 상의 원소를 아핀 변환하는 단계를 구비하는 것을 특징으로 하는 하드웨어 암호화/복호화 방법.

청구항 19

삭제

청구항 20

삭제

청구항 21

제 15항에 있어서, 상기 N개 키들 생성 단계는,

상기 입력키를 이용하여 상기 제1 라운드에서 사용될 상기 제1 키를 생성하는 단계; 및

이전 라운드에서 사용되는 키가 저장되는 레지스터 값을 이용하여, 상기 나머지 N-1 라운드들 각각에서 사용될 상기 제2 키 내지 상기 제N 키를 순차적으로 발생시키는 단계를 구비하고,

상기 입력키의 제공과 상기 제1 키의 발생은 소정 클럭의 한 싸이클에 이루어지는 것을 특징으로 하는 하드웨어 암호화/복호화 방법.

청구항 22

제14항에 있어서, 상기 2비트 데이터들의 승산은,

상기 상위 2비트 데이터의 상위 비트와 상기 하위 2비트 데이터의 상위 비트의 제1 논리곱을 구하는 단계;

상기 상위 2비트 데이터의 하위 비트와 상기 하위 2비트 데이터의 상위 비트의 제2 논리곱을 구하는 단계;

상기 상위 2비트 데이터의 상위 비트와 상기 하위 2비트 데이터의 하위 비트의 제3 논리곱을 구하는 단계;

상기 상위 2비트 데이터의 하위 비트와 상기 하위 2비트 데이터의 하위 비트의 제4 논리곱을 구하는 단계;

상기 제1 논리곱 및 상기 제2 논리곱의 제1 배타적 논리합을 구하는 단계;

상기 제1 배타적 논리합 및 상기 제3 논리곱의 제2 배타적 논리합을 상기 2비트 데이터들의 승산 결과의 상위 비트로 출력하는 단계; 및

상기 제1 논리곱 및 상기 제4 논리곱의 제3 배타적 논리합을 상기 2비트 데이터들의 승산 결과의 하위 비트로 출력하는 단계를 구비하는 것을 특징으로 하는 하드웨어 암호화/복호화 방법.

청구항 23

4비트 디지털 데이터의 하위 2비트와 상위 2비트 데이터를 제3 합산하는 제3 합산기;

갈로아 필드 GF(2^2) 상에서 상기 제3 합산 결과에 상기 하위 2비트 데이터를 제4 승산하는 제4 승산기;

상기 상위 2비트 데이터를 제2 자승하는 제2 자승기;

상기 제2 자승 결과에 제2 계수를 승산하는 제2 계수 승산기;

상기 제4 승산 결과와 상기 제2 계수 승산 결과를 제4 합산하는 제4 합산기;

상기 제4 합산 결과의 자승을 계산하여 상기 제4 합산 결과의 역원으로서 출력하는 제2 역원 계산기;

갈로아 필드 GF(2^2) 상에서 상기 제4 합산 결과의 역원에 상기 제3 합산 결과를 제5 승산하여, 상기 제5 승산 결과를 상기 하위 2비트 데이터의 역원으로서 출력하는 제5 승산기; 및

상기 갈로아 필드 GF(2^2) 상에서 상기 제4 합산 결과의 역원에 상기 상위 2비트 데이터를 제6 승산하여, 상기 제6 승산 결과를 상기 상위 2비트 데이터의 역원으로서 출력하는 제6 승산기를 포함하는 갈로아 필드 GF($(2^2)^2$) 상에서 4비트 디지털 데이터의 역원을 구하는 역원 계산기.

청구항 24

제 23항에 있어서, 상기 제4 승산기 내지 제6 승산기 각각은,

2개의 2비트 디지털 데이터들을 제1 데이터 및 제2 데이터로서 입력받아, 갈로아 필드 GF(2^2) 상에서 상기 2비트 데이터의 승산값을 계산하고,

상기 제1 데이터 및 상기 제2 데이터의 상위 비트 데이터를 제1 논리곱 연산하는 제1 논리곱 로직;

상기 제1 데이터의 하위 비트와 상기 제2 데이터의 상위 비트를 제2 논리곱 연산하는 제2 논리곱 로직;

상기 제1 데이터의 상위 비트와 상기 제2 데이터의 하위 비트를 제3 논리곱 연산하는 제3 논리곱 로직;

상기 제1 데이터 및 상기 제2 데이터의 하위 비트 데이터를 제4 논리곱 연산하는 제4 논리곱 로직;

상기 제1 논리곱 및 상기 제2 논리곱 연산 결과들을 제1 배타적 논리합 연산하는 제1 배타적 논리합 로직;

상기 제1 배타적 논리합 연산 결과와 상기 제3 논리곱 연산 결과를 제2 배타적 논리합 연산하여, 상기 제2 배타적 논리합 연산 결과를 상기 2비트 데이터의 승산값의 상위 비트 데이터로서 출력하는 제2 배타적 논리합 로직; 및

상기 제1 논리곱 및 상기 제4 논리곱 연산 결과들을 제3 배타적 논리합 연산하여, 상기 제3 배타적 논리합 연산 결과를 상기 2비트 데이터의 승산값의 하위 비트 데이터로서 출력하는 제3 배타적 논리합 로직을 포함하는 것을 특징으로 하는 역원 계산기.

청구항 25

갈로아 필드 GF(2^8) 상의원소를 갈로아 필드 GF($(((2^2)^2)^2$) 상의 원소로 변한한 뒤 합성 필드(Composite field)를 이용하여 원소의 곱셈의 역원을 계산하고, 상기 계산 결과를 이용하여 입력받는 벡터를 다른 벡터로 치환하는 S-BOX에 있어서,

상기 S-BOX는, 갈로아 필드 GF($(((2^2)^2)^2$) 상의 원소로부터 변환된 갈로아 필드 GF($(2^2)^2$) 상의 원소를 입력받아 GF($(2^2)^2$) 상에서 역원을 계산하는 제1 역원 계산기의 출력을 다시 GF($(((2^2)^2)^2$) 상의 원소로 변환하여 상기 원소의 곱셈의 역원을 계산하고,

상기 제1 역원 계산기는,

갈로아 필드 GF($(2^2)^2$) 상의 4비트 디지털 데이터의 하위 2비트와 상위 2비트 데이터를 제3 합산하는 제3 합산기;

갈로아 필드 GF(2^2) 상에서 상기 제3 합산 결과에 상기 하위 2비트 데이터를 제4 승산하는 제4 승산기;

상기 상위 2비트 데이터를 제2 자승하는 제2 자승기;

상기 제2 자승 결과에 제2 계수를 승산하는 제2 계수 승산기;

상기 제4 승산 결과와 상기 제2 계수 승산 결과를 제4 합산하는 제4 합산기;

상기 제4 합산 결과의 자승을 계산하여 상기 제4 합산 결과의 역원으로서 출력하는 제2 역원 계산기;

갈로아 필드 GF(2^2) 상에서 상기 제4 합산 결과의 역원에 상기 제3 합산 결과를 제5 승산하여, 상기 제5 승산 결과를 상기 하위 2비트 데이터의 역원으로서 출력하는 제5 승산기; 및

상기 갈로아 필드 GF(2^2) 상에서 상기 제4 합산 결과의 역원에 상기 상위 2비트 데이터를 제6 승산하여, 상기 제6 승산 결과를 상기 상위 2비트 데이터의 역원으로서 출력하는 제6 승산기를 포함하는 S-BOX.

청구항 26

제25항에 있어서, 상기 제4 승산기 내지 제6 승산기 각각은,

2개의 2비트 디지털 데이터들을 제1 데이터 및 제2 데이터로서 입력받아, 갈로아 필드 GF(2^2) 상에서 상기 2비트 데이터의 승산값을 계산하고,

상기 제1 데이터 및 상기 제2 데이터의 상위 비트 데이터를 제1 논리곱 연산하는 제1 논리곱 로직;

상기 제1 데이터의 하위 비트와 상기 제2 데이터의 상위 비트를 제2 논리곱 연산하는 제2 논리곱 로직;

상기 제1 데이터의 상위 비트와 상기 제2 데이터의 하위 비트를 제3 논리곱 연산하는 제3 논리곱 로직;

상기 제1 데이터 및 상기 제2 데이터의 하위 비트 데이터를 제4 논리곱 연산하는 제4 논리곱 로직;

상기 제1 논리곱 및 상기 제2 논리곱 연산 결과들을 제1 배타적 논리합 연산하는 제1 배타적 논리합 로직;

상기 제1 배타적 논리합 연산 결과와 상기 제3 논리곱 연산 결과를 제2 배타적 논리합 연산하여, 상기 제2 배타적 논리합 연산 결과를 상기 2비트 데이터의 승산값의 상위 비트 데이터로서 출력하는 제2 배타적 논리합 로직; 및

상기 제1 논리곱 및 상기 제4 논리곱 연산 결과들을 제3 배타적 논리합 연산하여, 상기 제3 배타적 논리합 연산 결과를 상기 2비트 데이터의 승산값의 하위 비트 데이터로서 출력하는 제3 배타적 논리합 로직을 포함하는 것을 특징으로 하는 S-BOX.

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

<15> 본 발명은 하드웨어 암호화/복호화 장치(cryptographic engine)에 관한 것으로, 특히 AES(Advanced Encryption Standard) 알고리즘의 하드웨어 암호화 또는 복호화 장치에 관한 것이다.

<16> 오늘날 스마트 카드, IC(Integrated Circuit) 카드 등을 통한 통신이나 인터넷 통신, 무선 랜(LAN) 통신 등에서, 유저(user)가 전송하는 정보에는 보안이 유지되어야 하는 비밀 정보가 상당히 많이 존재한다. 따라서, 유저의 비밀 정보가 해킹(hacking)에 의하여 유출되는 것을 방지하기 위하여, 서명이나 인증 절차를 밟아 전송되는 비밀 정보를 암호문으로 만들어 전송하는 하드웨어 암호화/복호화 장치가 필요하다.

<17> 암호화(encryption) 연산은 일반적으로 속도가 느리기 때문에, 스마트 카드와 같은 적용에서 하드웨어로 구현하는 경우가 많다. RSA(Rivest-Shamir-Adelman), ECC 체계(Elliptic Curve Crypto System) 등과 같은 공개키 알고리즘 뿐만 아니라 DES(Data Encryption Standard), AES(Advanced Encryption Standard)와 같은 대칭키 알고리즘도 하드웨어로 구현된다.

<18> 특히, AES는 SPN(Substitution Permutation Network) 구조를 가지고, 이는 DES를 대치하는 대칭키 암호화 알고리즘으로써, 블록의 길이는 128비트이고, 키(Key) 길이는 128, 192, 및 256 비트를 사용한다. 사용되는 키 길이 각각에 따라 10, 12, 및 14 라운드를 수행한다. AES의 암호화 과정은, 초기 입력키 합산 및 각 라운드의 연산으

로 이루어진다. 예를 들어, AES에서 암호화 과정시 사용되는 라운드 수를 Nr이라 하면, "Sub_Byte 변환(transformation)", "Shift_Row 변환", "Mix_Column 변환", 및 "Add_Round_Key 연산"으로 이루어진 라운드 연산이 (Nr-1)번 수행되고, 최종 라운드 연산에서는 "Mix_Column 변환"을 제외한 "Sub_Byte 변환", "Shift_Row 변환", 및 "Add_Round_Key 연산"이 1번 수행된다. 따라서, 종래의 AES 암호화 알고리즘의 구현에서, 암호화 과정에는 (Nr+1) 이상의 클럭 싸이클이 요구되고, 암호화 과정의 역과정을 수행하는 복호화(decryption) 과정에는 2(Nr+1) 이상의 클럭 싸이클이 요구된다. 이와 같은 AES 암호화 알고리즘의 라운드 연산에 대하여 미국 공개 특허, "US2003-0133568" 또는 한국 공개 특허, "KR2002-61718"에 잘 나타나 있다.

<19> 그런데, 비선형(non-linear) 변환인 "Sub_Byte 변환"은 S-BOX에 의하여 이루어지고, S-BOX의 연산은 AES 구현시 가장 많은 전력을 소모한다. 즉, S-BOX는 비선형 변환 함수로써 입력 데이터를 다른 데이터로 치환하고, 이때, 비선형 변환 함수의 연산을 위하여 사용되는 메모리와 회로의 복잡도가 커서 많은 전력을 소모한다. 예를 들어, S-BOX에서 비선형 함수에 따른 치환 연산의 수행을 위하여, 룩업 테이블(Look-up Table), SOP(Sum-of-Products), POS(Produce-of-Sum), PPRM(Positive Polarity Reed-Muller) form, BDD(Binary Decision Diagram) 등 다양한 방법들이 적용된다. S-BOX의 입력값에 대한 변환값을 얻기 위하여, 룩업 테이블(Look-up Table) 방식은 ROM(Read Only Memory)에 그 값들을 저장하여 참조한다. SOP, POS, PPRM form, BDD 등의 방식은 데이터들을 8개의 입력에 의한 이진(binary) 표현으로 나타내어 회로를 구현한다. 이때, 이러한 종래의 방식으로 S-BOX를 구현하면, 800~2200개 정도의 게이트(gate) 사이즈가 요구되어, 스마트 카드, IC 카드 등과 같이 메모리 및 대역폭에 제한이 있고, 저전력 및 빠른 처리 속도가 요구되는 소형 시스템에 적합하지 않다는 문제점이 있다.

발명이 이루고자 하는 기술적 과제

<20> 따라서, 본 발명이 이루고자하는 기술적 과제는, 스마트 카드나 IC 카드 등 소형 시스템에 용이하게 적용할 수 있는 저전력 및 고속의 암호화 또는 복호화가 가능한 하드웨어 암호화/복호화 장치를 제공하는 데 있다.

<21> 본 발명이 이루고자하는 다른 기술적 과제는, 저전력 및 고속의 암호화 또는 복호화가 가능한 하드웨어 암호화/복호화 방법을 제공하는 데 있다.

발명의 구성 및 작용

<22> 상기의 기술적 과제를 달성하기 위한 본 발명에 따른 하드웨어 암호화/복호화 장치는, 라운드 연산부,및 키 스케쥴러를 구비하는 것을 특징으로 한다. 상기 라운드 연산부는 각 라운드에 해당하는 N개의 키들을 입력받아, 제1 라운드에서 상기 키들 중 제1 키를 이용하여 입력 데이터를 암호문으로 변환하고, 나머지 N-1 라운드 각각에서 순차적으로 상기 키들 중 제2 키 내지 제N 키를 이용하여 이전 라운드의 변환 결과를 다른 암호문으로 변환한다. 상기 키 스케쥴러는 입력키를 이용하여 상기 제1 키 내지 상기 제N 키 각각을 생성한다. 상기 라운드 각각의 S-BOX은, 갈로아 필드 $GF(2^8)$ 상의 원소를 갈로아 필드 $GF(((2^2)^2)^2)$ 상의 원소로 변환한 뒤 합성 필드(Composite)를 이용하여 원소의 곱셈의 역원을 계산하고, 상기 계산 결과를 이용하여 입력받는 벡터를 다른 벡터로 치환하는 것을 특징으로 한다. 상기 하드웨어 암호화/복호화 장치는, 전송할 데이터와 상기 입력키를 합산하여, 그 합산 결과를 상기 입력 데이터로서 출력하는 합산기를 더 구비하는 것을 특징으로 한다.

<23> 상기 S-BOX는, 델타 변환부, 역원 계산부, 역 델타 변환부, 및 아핀 변환부를 구비하는 것을 특징으로 한다. 상기 델타 변환부는 입력받는 벡터의 각 원소를 이루는 갈로아 필드 $GF(2^8)$ 상의 원소를 갈로아 필드 $GF(((2^2)^2)^2)$ 상의 원소로 변환한다. 상기 역원 계산부는 상기 갈로아 필드 $GF(((2^2)^2)^2)$ 상의 원소의 역원을 계산하여 출력한다. 상기 역 델타 변환부는 상기 갈로아 필드 $GF(((2^2)^2)^2)$ 상의 원소의 역원을 갈로아 필드 $GF(2^8)$ 상의 원소로 변환한다. 상기 아핀 변환부는 아핀 함수에 따라 상기 변환된 갈로아 필드 $GF(2^8)$ 상의 원소를 아핀 변환한다.

<24> 상기의 기술적 과제를 달성하기 위한 본 발명에 따른 하드웨어 암호화/복호화 방법은, N개의 라운드들에 대응하는 해당 N개의 키들을 입력받는 단계; 상기 라운드들 중 제1 라운드에서 상기 키들 중 제1 키를 이용하여 입력 데이터를 암호문으로 변환하는 단계; 나머지 N-1 라운드들 각각에서 순차적으로 상기 키들 중 제2 키 내지 제N 키를 이용하여 이전 라운드의 변환 결과를 다른 암호문으로 변환하는 단계; 및 입력키를 이용하여 상기 제1 키 내지 상기 제N 키 각각을 생성하는 단계를 구비하고, 상기 라운드들 각각의 암호문으로 변환 단계는, S-BOX 연산에서, 갈로아 필드 $GF(2^8)$ 상의 원소를 갈로아 필드 $GF(((2^2)^2)^2)$ 상의 원소로 변환한 뒤 합성 필드(Composite)를 이용하여 원소의 곱셈의 역원을 계산하고, 입력받는 벡터를 상기 계산 결과를 이용하여 다른 벡

터로 치환하는 단계를 구비하는 것을 특징으로 한다. 상기 하드웨어 암호화/복호화 방법은, 전송할 데이터와 상기 입력키를 합산하여, 그 합산 결과를 상기 입력 데이터로서 출력하는 단계를 더 구비하는 것을 특징으로 한다.

<25> 본 발명과 본 발명의 동작상의 이점 및 본 발명의 실시에 의하여 달성되는 목적을 충분히 이해하기 위해서는 본 발명의 바람직한 실시예를 예시하는 첨부 도면 및 첨부 도면에 기재된 내용을 참조하여야만 한다.

<26> 이하, 첨부한 도면을 참조하여 본 발명의 바람직한 실시예를 설명함으로써, 본 발명을 상세히 설명한다. 각 도면에 제시된 동일한 참조부호는 동일한 부재를 나타낸다.

<27> 도 1은 본 발명의 일실시예에 따른 하드웨어 암호화 장치(100)의 블록도이다. 도 1을 참조하면, 본 발명의 일실시예에 따른 AES 방식의 하드웨어 암호화 장치(100)는, 합산기(110), 및 라운드 연산을 수행하는 다수의 N개의 라운드들(120~150)을 구비한다. 이외에도, 상기 하드웨어 암호화 장치(100)는, 도 4에 도시된 바와 같은 키 스케쥴러(key scheduler)(400)를 구비한다. 상기 키 스케쥴러(400)는 입력키(INKEY)와 상기 다수의 N개 라운드들(120~150)에 해당키들(KEY1~KEY10)을 제공한다. 상기 키 스케쥴러(400)에 대해서는 도 4의 설명에서 좀더 자세히 설명된다. 상기 다수의 N개 라운드들(120~150) 각각에서의 라운드 연산은, 각 라운드에서 중복되는 연산이 공유될 수 있다.

<28> 상기 합산기(110)는 초기 입력키(INKEY) 합산을 수행한다. 즉, 상기 합산기(110)는 전송할 데이터(TXD)와 상기 입력키(INKEY)를 합산하여, 그 합산 결과를 라운드들(120~150) 중 제1 라운드(120)의 입력 데이터로서 출력한다. 여기서, 전송할 데이터(TXD)의 블록 길이는, 일반적인 경우와 마찬가지로 128 비트인 것으로 가정된다.

<29> 상기 다수의 N개 라운드들(120~150)은 각 라운드에 해당하는 N개의 키들(KEY1~KEY10)을 입력받아, 암호화를 위한 라운드 연산을 수행한다. 여기서, 키들(KEY1~KEY10) 각각의 데이터 길이는 128 비트인 것으로 가정하고, 이에 따라 라운드들(120~150)의 수는 10개이고 10 라운드 연산을 수행하는 것으로 가정된다. 이외에도, 주지된 바와 같이, 키 길이가 192, 및 256 비트 각각인 경우에는 12 및 14 라운드 연산을 수행한다.

<30> 상기 라운드들(120~150) 중 제1 라운드(120)는 상기 키들 중 제1 키(KEY1)를 이용하여 입력 데이터(TXD + INKEY)를 암호문으로 변환한다. 이에 따라, 나머지 9 라운드들(130~150) 각각은 순차적으로 상기 키들 중 제2 키(KEY2) 내지 제10 키(KEY10)를 이용하여 이전 라운드의 변환 결과를 다른 암호문으로 변환한다. 제10번째 최종 라운드(150)는 제10 키(KEY10)를 이용하여 제9 라운드(140)의 변환 결과를 최종 암호문(CIPHD)으로 변환한다. 이와 같이 전송할 데이터(TXD)가 암호화된 최종 암호문(CIPHD)은 스마트 카드, IC(Integrated Circuit) 카드 등과 같은 소형 시스템에서 전송되는 비밀 정보가 된다. 이외에도 상기 AES 방식의 하드웨어 암호화/복호화 장치는 보안이 유지되어야 하는 비밀 정보의 송수신을 위하여, 인터넷 통신, 무선 랜(LAN) 통신 등에도 이용될 수 있다.

<31> 여기서, 상기 라운드들(120~150)에 의하여, 일반적인 AES 암호화 과정과 마찬가지로, 라운드 수가 10이므로, "Sub_Byte 변환(transformation)", "Shift_Row 변환", "Mix_Column 변환", 및 "Add_Round_Key 연산"으로 이루어진 라운드 연산이 9번 수행되고, 최종 라운드 연산에서는 "Mix_Column 변환"을 제외한 "Sub_Byte 변환", "Shift_Row 변환", 및 "Add_Round_Key 연산"이 1번 수행된다. 일반적으로, 비선형(non-linear) 변환인 "Sub_Byte 변환"을 수행하기 위해서는 사용되는 메모리와 회로의 복잡도가 커서 많은 전력을 소모한다. 이에 따라, 본 발명의 일실시예에 따른 하드웨어 암호화/복호화 장치는, 라운드 연산에서 Sub_Byte 회로(도 2의 160, 도 3의 200) 또는 역 Sub_Byte 회로(도 11의 1700, 도 12의 2100)에 새로운 S-BOX(도 5 및 도 13)를 구비하여, 종래와 다른 방식으로 "Sub_Byte 변환"과 "역 Sub_Byte 변환"을 수행하여 입력받는 벡터를 다른 벡터로 치환한다. 먼저, 본 발명의 일실시예에 따라 제안된 하드웨어 암호화 장치(100)에서는, 상기 라운드들(120~150)의 라운드 연산 수행 시 S-BOX(도 5)의 하드웨어 부담을 줄이고 소비 전력을 줄이기 위하여, "Sub_Byte 변환"의 수행에서 갈로아 필드(Galois Field) $GF(2^8)$ 상의 원소의 곱셈의 역원 계산(multiplicative inverse)이 갈로아 필드 GF(2)의 합성 필드(composite field)들, 즉, $GF(2^2)$, $GF((2^2)^2)$, 및 $GF(((2^2)^2)^2)$ 상의 연산으로 이루어진다. 곱셈의 역원은 곱하여 1로 만드는 수로서 역수(reciprocal number)이다. 본 발명의 일실시예에 따라 제안된 S-BOX(도 5)의 동작에 대해서는 도 2, 도 3, 및 도 5의 설명에서 좀더 구체적으로 기술된다.

<32> 도 2는 도 1의 제1 라운드(120) 내지 제9 라운드(140)를 나타내는 구체적인 블록도이다. 도 2를 참조하면, 제1 라운드(120) 내지 제9 라운드(140) 각각은, Sub_Byte 회로(160), Shift_Row 회로(170), Mix_Column 회로(180), 및 합산기(190)를 구비한다. 위에서 기술한 바와 같이, 라운드 수가 10이므로, 상기 제1 라운드(120) 내지 상기

제9 라운드(140)를 통하여, "Sub_Byte 변환(transformation)", "Shift_Row 변환", "Mix_Column 변환", 및 "Add_Round_Key 연산"으로 이루어진 라운드 연산이 9번 수행된다.

<33> 상기 Sub_Byte 회로(160)는, S-BOX(도 5)를 통하여, "Sub_Byte 변환(transformation)"을 위한 갈로아 필드 $GF(2^8)$ 상의 역원 계산에서, 갈로아 필드 $GF(((2^2)^2)^2)$ 상의 연산을 이용하여 계산하고, 상기 계산 결과를 이용하여 입력받는 벡터(INCIPH)를 다른 벡터로 치환한다. 즉, 갈로아 필드(Galois Field) $GF(2^8)$ 상의 역원 계산은 갈로아 필드 GF(2)의 합성 필드들, 즉, $GF(2^2)$, $GF((2^2)^2)$, 및 $GF(((2^2)^2)^2)$ 상의 연산으로 이루어진다.

<34> 이와 같은 합성 필드를 이용하여 역원을 계산하는 이론에 대해서는, 논문, "Akashi Satoh, Sumio Morioka, Kohji Takano, and Seiji Munetoh, <A Compact Rijndael Hardware Architecture with S-Box Optimization>, ASIACRYPT 2001"이 참조되었다. 일반적인 통신 표준에 따르면, 갈로아 필드 $GF(2^8)$, $GF(2^2)$, $GF((2^2)^2)$, 및 $GF(((2^2)^2)^2)$ 각각에 대한 원시 다항식(primitive polynomial)은 [수학식 1]과 같다. [수학식 1]과 같은 원시 다항식은 약분될 수 없는 기약 다항식(irreducible polynomial)이다. $\lambda=\{1100\}_2 \in GF((2^2)^2)$이고, $\emptyset=\{10\}_2 \in GF(2^2)$이다. 즉, 제1 계수 λ는 갈로아 필드 $GF((2^2)^2)$ 상에서 이진수 $\{1100\}_2$ 이고, 제2 계수 ø는 갈로아 필드 $GF(2^2)$ 상에서 이진수 $\{10\}_2$ 이다.

<35> [수학식 1]

$$GF(2^8): x^8+x^4+x^3+x+1$$

$$GF(2^2): x^2+x+1$$

$$GF((2^2)^2): x^2+x+\emptyset$$

<36> $$GF(((2^2)^2)^2): x^2+x+\lambda$$

<37> 상기 Shift_Row 회로(170)는 "Shift_Row 변환"을 수행하기 위하여, 상기 Sub_Byte 회로(160)의 출력 신호를 입력 벡터로 받아, 로우 단위로 쉬프트 처리하는 함수에 따라 상기 입력 벡터를 로우 단위로 쉬프트 처리하여 출력한다. 상기 Mix_Column 회로(180)는 "Mix_Column 변환"을 수행하기 위하여, 컬럼 단위로 치환 처리하는 함수에 따라 상기 Shift_Row 회로(170)의 출력 벡터를 컬럼 단위로 치환 처리하여 출력한다. 상기 합산기(190)는 "Add_Round_Key 연산"을 수행하기 위하여, 상기 Mix_Column 회로(180)의 출력 벡터와 상기 키들 중 해당 라운드 키(KEYN)를 합산하여 출력한다. 상기 합산기(190)에서 출력된 암호문(OUTCIPH)은 다음 라운드 의 입력이 된다.

<38> 도 3은 도 1의 제10 라운드(150)를 나타내는 구체적인 블록도이다. 도 3을 참조하면, 도 1의 제10 라운드(150)는 Sub_Byte 회로(200), Shift_Row 회로(210), 및 합산기(220)를 구비한다. 위에서 기술한 바와 같이, 라운드 수가 10이므로, 최종 라운드인 상기 제10 라운드(150)를 통하여, "Sub_Byte 변환(transformation)", "Shift_Row 변환", 및 "Add_Round_Key 연산"으로 이루어진 라운드 연산이 1번 수행된다. 상기 Sub_Byte 회로(200), 상기 Shift_Row 회로(210), 및 상기 합산기(220)의 동작은 도 2의 Sub_Byte 회로(160), Shift_Row 회로(170), 및 합산기(190)의 동작과 같으므로 여기서는 설명을 생략한다.

<39> 도 4는 도 1의 키들(INKEY, KEY1~KEY10)을 발생시키는 키 스케쥴러(400)를 나타내는 블록도이다. 도 4를 참조하면, 상기 키 스케쥴러(400)는 레지스터(410), 먹스(multiplexer)(420), 및 키 생성기(key generator)(430)를 구비한다.

<40> 도 4에서, 입력키(INKEY)는 유저가 암호화에 사용하는 키로서, 본 발명에 따른 AES 암호화 과정을 위하여 유저에 의하여 입력되는 키이다. 상기 키 생성기(430)는 상기 먹스(420)를 통하여 입력되는 상기 입력키(INKEY)를 이용하여 상기 제1 라운드(120)에서 사용될 제1 키(KEY1)를 생성한다. 상기 키 스케쥴러(400)는 제1 라운드(120)의 연산이 이루어지기 전인 초기에, 도 1의 합산기(110)에 상기 입력키(INKEY)를 제공한다. 도 1의 합산기(110)에 상기 입력키(INKEY)의 제공과 상기 키 생성기(430)에서의 상기 제1 키(KEY1)의 발생은 시스템 클럭(미

도시)의 한 싸이클에 이루어질 수 있다. 상기 키 생성기(430)에서 생성된 상기 제1 키(KEY1)는 상기 레지스터(410)에 저장되고 동시에 제1 라운드(120)의 라운드 키가되며, 다음 시스템 클럭에 상기 레지스터(410)로부터 상기 먹스(420)로 입력된다. 상기 먹스(420)는 상기 소정 제어 신호(RNDST)의 논리 상태에 따라, 선택적으로 입력키(INKEY) 또는 상기 레지스터(410)에서 출력된 상기 제1 키(KEY1)를 출력한다. 상기 제1 키(KEY1)가 상기 키 생성기(430)의 입력이 되면, 상기 키 생성기(430)는 제2 키(KEY2)를 생성하여 출력한다.

<41> 즉, 나머지 9 라운드들(130~150) 각각에서 사용될 제2 키(KEY2) 내지 제10 키(KEY10)는, 상기 키 생성기(430)가 이전 라운드에서 사용되는 키(KEYN)가 저장되는 상기 레지스터(410)의 값을 이용하여 순차적으로 발생시킨다. 예를 들어, 상기 제1 키(KEY1)가 상기 레지스터(410)로부터 상기 먹스(420)를 통하여 상기 키 생성기(430)에 입력될 때, 상기 키 생성기(430)는 상기 제1 키(KEY1)를 이용하여 제2 라운드(130)에서 사용될 제2 키(KEY2)를 발생시킨다.

<42> 이와 같이 상기 키 스케쥴러(400)가 입력키(INKEY)를 이용하여 상기 제1 키(KEY1) 내지 상기 제10 키(KEY10) 각각을 생성함으써, 10개 라운드들(120~150)에 해당 라운드키들(KEY1~KEY10)을 제공한다. 위에서 기술한 바와 같이, 도 1의 합산기(110)에 상기 입력키(INKEY)의 제공과 상기 제1 키(KEY1)의 발생은 시스템 클럭의 한 싸이클에 이루어지므로, 도 1과 같은 본 발명에 따른 AES 암호화 알고리즘의 구현에서, 암호화 과정에는 10 클럭 싸이클이 요구된다. 암호화 과정의 역과정을 수행하는 복호화 과정에는 20 클럭 싸이클이 요구된다. 이와 같이, 본 발명의 AES 암호화 과정에서는 키 발생 클럭 싸이클 수를 최소화하여 빠른 연산이 이루어지도록 하였다. 복호화 과정에 관하여는 도 10 내지 도 13의 설명에서 좀 더 구체적으로 설명된다.

<43> 도 5는 도 2 및 도 3의 Sub_Byte 회로(160, 200)에서 사용되는 S-BOX를 나타내는 블록도이다. 도 5를 참조하면, 상기 S-BOX는 델타 변환부(δ:isomorphic transformation unit)(161), 역원 계산부(inverse operation unit)(162), 역 델타 변환부(δ^{-1}:inverse isomorphic transformation unit)(163), 및 아핀 변환부(affine transformation unit)(164)를 구비한다.

<44> 상기 델타 변환부(161)는 입력받는 벡터(SBIN)의 각 원소를 이루는 갈로아 필드 $GF(2^8)$ 상의 원소를 갈로아 필드 $GF(((2^2)^2)^2)$ 상의 원소로 동형 변환(isomorphic transformation)한다. 도 5에 도시된 바와 같이, 입력받는 벡터(SBIN)는 128 비트이고, 이들은 8 비트의 데이터를 가지는 16 원소들(S00~S33)로 이루어진다. 상기 델타 변환부(161)의 동형 변환(isomorphic transformation) 식은 [수학식 2] 및 [수학식 3]과 같다. [수학식 2]에서, x는 입력 벡터(SBIN)이고, y는 동형 변환(isomorphic transformation) 벡터 δ에 의하여 변환된 벡터이다.

<45> [수학식 2]

<46> $y=\delta * x$

<47> [수학식 3]

<48>
$$\delta = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$

<49> 상기 역원 계산부(162)는 상기 갈로아 필드 $GF(((2^2)^2)^2)$ 상의 원소의 곱셈의 역원을 계산하여 출력한다. 상기 역원 계산부(162)의 역원 계산은 도 6에서 자세히 설명된다.

<50> 상기 역 델타 변환부(163)는 상기 역원 계산부(162)에서 계산된 상기 갈로아 필드 $GF(((2^2)^2)^2)$ 상의 원소의 곱셈의 역원을 갈로아 필드 $GF(2^8)$ 상의 원소로 역 동형 변환(inverse isomorphictransformation)한다. 상기 역 델타 변환부(163)의 역 동형 변환(inverse isomorphic transformation) 식은 [수학식 4] 및 [수학식 5]와

같다. [수학식 4]에서, y는 상기 역 델타 변환부(163)가 입력받는 역원 벡터이고, x는 역 동형 변환(inverse isomorphic transformation) 벡터 δ^{-1}에 의하여 역 변환된 벡터이다.

<51> [수학식 4]

<52> $x=\delta^{-1}*y$

<53> [수학식 5]

<54>
$$\delta^{-1}=\begin{bmatrix}1&0&1&0&1&1&1&0\\0&0&0&0&1&1&0&0\\0&1&1&1&1&0&0&1\\0&1&1&1&1&1&0&0\\0&1&1&0&1&1&1&0\\0&1&0&0&0&1&1&0\\0&0&1&0&0&0&1&0\\0&1&0&0&0&1&1&1\end{bmatrix}$$

<55> 상기 아핀 변환부(164)는 아핀 함수에 따라 상기 역 델타 변환부(163)에서 변환된 갈로아 필드 GF(2^8) 상의 원소를 아핀 변환한다. 도 5에 도시된 바와 같이, 아핀 변환된 벡터(SBOUT)는 상기 델타 변환부(161)가 입력받는 벡터(SBIN)와 마찬가지로 128 비트이고, 이들은 8 비트의 데이터를 가지는 16 원소들(S00'~S33')로 이루어진다. 아핀 변환 식은 [수학식 6]과 같다. [수학식 6]에서 x_0~x_7은 상기 역 델타 변환부(163)에서 변환된 갈로아 필드 GF(2^8) 상의 원소(8비트 데이터)의 비트 값이고, x'_0~x'_7은 아핀 변환된 원소(8비트 데이터)의 비트 값이다.

<56> [수학식 6]

<57>
$$\begin{bmatrix}x'_0\\x'_1\\x'_2\\x'_3\\x'_4\\x'_5\\x'_6\\x'_7\end{bmatrix}=\begin{bmatrix}1&0&0&0&1&1&1&1\\1&1&0&0&0&1&1&1\\1&1&1&0&0&0&1&1\\1&1&1&1&0&0&0&1\\1&1&1&1&1&0&0&0\\0&1&1&1&1&1&0&0\\0&0&1&1&1&1&1&0\\0&0&0&1&1&1&1&1\end{bmatrix}\begin{bmatrix}x_0\\x_1\\x_2\\x_3\\x_4\\x_5\\x_6\\x_7\end{bmatrix}+\begin{bmatrix}1\\1\\0\\0\\0\\1\\1\\0\end{bmatrix}$$

<58> 도 6은 GF((((2^2)^2)^2) 상에서 역원 계산을 위한 도 5의 역원 계산부(162)를 나타내는 구체적인 블록도이다. 도 6을 참조하면, 상기 역원 계산부(162)는 제1 합산기(601), 제1 승산기(602), 제1 자승기(603), 제1 계수 승산기(608), 제2 합산기(604), 제1 역원 계산기(605), 제2 승산기(606), 및 제3 승산기(607)를 구비한다. 상기 제1 합산기(601)는 상기 갈로아 필드 GF((((2^2)^2)^2) 상의 원소를 이루는 8비트 디지털 데이터의 하위 4비트 데이터 P_L[3:0]과 상위 4비트 데이터 P_H[3:0]를 제1 합산한다. 상기 제1 승산기(602)는 갈로아 필드 GF((2^2)^2) 상에서 상기 제1 합산 결과에 상기 하위 4비트 데이터 P_L[3:0]를 제1 승산한다. 상기 제1 자승기(603)는 상기 상위 4비트 데이터 P_H[3:0]를 제1 자승(square)한다. 상기 제1 계수 승산기(608)는 상기 제1 자승 결과에 제1 계수(λ)([수학식 1] 참조)를 승산한다. 상기 제2 합산기(604)는 상기 제1 승산 결과와 상기 제1 자승 결과를 제2 합산한다. 상기 제1 역원 계산기(605)는 상기 갈로아 필드 GF((2^2)^2) 상에서 상기 제2 합산 결과의 역원을 계산한다. 상기 제1 역원 계산기(605)의 역원 계산에 대해서는 도 7의 설명에서 자세히 기술된다.

<59> 상기 제2 승산기(606)는 갈로아 필드 GF((2^2)^2) 상에서 상기 제2 합산 결과의 역원에 상기 제1 합산 결과를 제2

승산하여, 상기 제2 승산 결과를 상기 하위 4비트 데이터의 역원 P_L^{-1}[3:0]으로서 출력한다. 상기 제3 승산기(607)는 갈로아 필드 GF($(2^2)^2$) 상에서 상기 제2 합산 결과의 역원에 상기 상위 4비트 데이터 P_H[3:0]를 제3 승산하여, 상기 제3 승산 결과를 상기 상위 4비트 데이터의 역원 P_H^{-1}[3:0]으로서 출력한다.

<60> 도 7은 GF($(2^2)^2$) 상에서 역원 계산을 위한 도 6의 제1 역원 계산기(605)를 나타내는 구체적인 블록도이다. 도 7을 참조하면, 도 6의 제1 역원 계산기(605)는 제3 합산기(701), 제4 승산기(702), 제2 자승기(703), 제2 계수 승산기(704), 제4 합산기(705), 제2 역원 계산기(706), 제5 승산기(707), 및 제6 승산기(708)를 구비한다. 상기 제3 합산기(701)는 도 6의 제2 합산기(604)에서 출력되는 제2 합산 결과를 이루는 4비트 디지털 데이터의 하위 2비트 데이터 Q_L[1:0]와 상위 2비트 데이터 Q_H[1:0]를 제3 합산한다. 상기 제4 승산기(702)는 갈로아 필드 GF(2^2) 상에서 상기 제3 합산 결과에 상기 하위 2비트 데이터 Q_L[1:0]를 제4 승산한다. 상기 제2 자승기(703)는 상기 상위 2비트 데이터 Q_H[1:0]를 제2 자승한다. 상기 제2 계수 승산기(704)는 상기 제2 자승 결과에 제2 계수(ø)([수학식 1] 참조)를 승산한다. 상기 제4 합산기(705)는 상기 제4 승산 결과와 상기 제2 계수 승산 결과를 제4 합산한다. 상기 제2 역원 계산기(706)는 상기 제4 합산 결과의 자승(square)을 계산하여 상기 제4 합산 결과의 역원으로서 출력한다. 즉, 상기 제4 합산 결과의 자승은 그 역원과 같다. 상기 제5 승산기(707)는 갈로아 필드 GF(2^2) 상에서 상기 제4 합산 결과의 역원에 상기 제3 합산 결과를 제5 승산하여, 상기 제5 승산 결과를 상기 하위 2비트 데이터의 역원 Q_L^{-1}[1:0]으로서 출력한다. 상기 제6 승산기(708)는 상기 갈로아 필드 GF(2^2) 상에서 상기 제4 합산 결과의 역원에 상기 상위 2비트 데이터를 제6 승산하여, 상기 제6 승산 결과를 상기 상위 2비트 데이터의 역원 Q_H^{-1}[1:0]으로서 출력한다.

<61> 도 8은 GF($(2^2)^2$) 상에서 승산을 위한 도 6의 4비트 승산기(602, 606, 607)를 나타내는 구체적인 블록도이다. 도 8을 참조하면, 도 6의 4비트 승산기(602, 606, 607)는, 제5 합산기(801), 제6 합산기(802), 제7 승산기(803), 제8 승산기(804), 제9 승산기(805), 제7 합산기(806), 제3 계수 승산기(807), 및 제8 합산기(808)를 구비한다. 상기 4비트 승산기(602, 606, 607)는 2개의 4비트 디지털 데이터들을 제1 데이터(A) 및 제2 데이터(B)로서 입력받아, 갈로아 필드 GF($(2^2)^2$) 상에서 상기 2개의 4비트 데이터의 승산값(M)을 계산한다. 상기 제5 합산기(801)는 상기 제2 데이터(B)의 하위 2비트 데이터 B_L[1:0]와 상위 2비트 데이터 B_H[1:0]를 제5 합산한다. 상기 제6 합산기(802)는 상기 제1 데이터(A)의 하위 2비트 A_L[1:0]와 상위 2비트 데이터 A_H[1:0]를 제6 합산한다. 상기 제7 승산기(803)는 갈로아 필드 GF(2^2) 상에서 상기 제2 데이터(B)의 하위 2비트 데이터 B_L[1:0] 및 상기 제1 데이터(A)의 하위 2비트 데이터 A_L[1:0]를 제7 승산한다. 상기 제8 승산기(804)는 상기 제2 데이터(B)의 상위 2비트 데이터 B_H[1:0] 및 상기 제1 데이터(A)의 상위 2비트 데이터 A_H[1:0]를 제8 승산한다. 상기 제9 승산기(805)는 상기 갈로아 필드 GF(2^2) 상에서 상기 제5 합산 결과에 상기 제6 합산 결과를 제9 승산한다. 상기 제7 합산기(806)는 상기 제9 승산 결과와 상기 제7 승산 결과를 제7 합산하여, 상기 제7 합산 결과를 상기 4비트 데이터의 승산값의 상위 2비트 데이터 M_H[1:0]로서 출력한다. 상기 제3 계수 승산기(807)는 상기 제8 승산 결과에 상기 제2 계수(ø)([수학식 1] 참조)를 승산한다. 상기 제8 합산기(808)는 상기 제7 승산 결과와 제2 계수 승산 결과를 제8 합산하여, 상기 제8 합산 결과를 상기 4비트 데이터의 승산값의 하위 2비트 데이터 M_L[1:0]로서 출력한다.

<62> 도 9는 GF(2^2) 상에서 승산을 위한 도 7 및 도 8의 2비트 승산기(702, 707, 708, 803, 804, 805)를 나타내는 구체적인 블록도이다. 도 9를 참조하면, 도 7 및 도 8의 2비트 승산기(702, 707, 708, 803, 804, 805)는, 제1 논리곱(AND) 로직(901), 제2 논리곱 로직(902), 제3 논리곱 로직(903), 제4 논리곱 로직(904), 제1 배타적 논리합(Exclusive OR) 로직(905), 제2 배타적 논리합 로직(906), 및 제3 배타적 논리합 로직(907)을 구비한다. 상기 2비트 승산기(702, 707, 708, 803, 804, 805)는 2개의 2비트 디지털 데이터들을 제3 데이터(C) 및 제4 데이터(D)로서 입력받아, 갈로아 필드 GF(2^2) 상에서 상기 2개의 2비트 데이터(C, D)의 승산값을 계산한다. 상기 2개의 2비트 데이터(C, D)의 승산값의 계산은, [수학식 7]을 이용한다. 즉, 제3 데이터(C)를 ax+b, 제4 데이터

(D)를 cx+d로 나타내면, [수학식 7]이 성립한다. [수학식 1]에서, 갈로아 필드 GF(2^2) 상에서 원시 다항식은 x^2+x+1이고, 이 원시 다항식은 약분될수 없는(irreducible) 기약 다항식이므로, [수학식 7]에서처럼 x^2은 x+1과 같다. [수학식 7]에서 a, c는 2비트 데이터 중 상위 비트 데이터이고, b, d는 2비트 데이터 중 하위 비트 데이터이다.

<63> [수학식 7]

<64> $(ax + b)(cx + d) = acx^2 + adx + bcx + bd$

<65> $= ac(x + 1) + adx + bcx + bd$

<66> $= (ac + ad + bc)x + (ac + bd)$

<67> 따라서, 상기 2비트 승산기(702, 707, 708, 803, 804, 805)는 다음과 같이 승산값을 계산한다. 상기 제1 논리곱 로직(901)은 상기 제3 데이터(C) 및 상기 제4 데이터(D)의 상위 비트 데이터(a, c)를 제1 논리곱 연산한다. 상기 제2 논리곱 로직(902)은 상기 제3 데이터(C)의 하위 비트(b)와 상기 제4 데이터(D)의 상위 비트(c)를 제2 논리곱 연산한다. 상기 제3 논리곱 로직(903)은 상기 제3 데이터(C)의 상위 비트(a)와 상기 제4 데이터(D)의 하위 비트(d)를 제3 논리곱 연산한다. 상기 제4 논리곱 로직(904)은 상기 제3 데이터(C) 및 상기 제4 데이터(D)의 하위 비트 데이터(b, d)를 제4 논리곱 연산한다. 상기 제1 배타적 논리합 로직(905)은 상기 제1 논리곱 연산 결과(ac)및 상기 제2 논리곱 연산 결과(bc)를 제1 배타적 논리합 연산한다. 상기 제2 배타적 논리합 로직(906)은 상기 제1 배타적 논리합 연산 결과와 상기 제3 논리곱 연산 결과(ad)를 제2 배타적 논리합 연산하여, 상기 제2 배타적 논리합 연산 결과를 상기 2비트 데이터의 승산값의 상위 비트 데이터(ac+ad+bc)로서 출력한다. 상기 제3 배타적 논리합 로직(907)은 상기 제1 논리곱 연산 결과(ac)및 상기 제4 논리곱 연산 결과(bd)를 제3 배타적 논리합 연산하여, 상기 제3 배타적 논리합 연산 결과를 상기 2비트 데이터의 승산값의 하위 비트 데이터(ac+bd)로서 출력한다.

<68> 도 10은 도 1의 하드웨어 암호화 장치(100)로부터 전송된 암호문을 복호하는 하드웨어 복호화(decryption) 장치를 나타내는 일례이다. 도 10에 도시된 바와 같이, 수신측에서 하드웨어 복호화 장치는 도 1의 하드웨어 암호화 장치(100)에서 전송된 암호문(CIPHD)을 수신하고, 유저로부터 입력받는 입력키(INKEY)를 이용하여 암호문(CIPHD)을 평문(plain text)으로 복호한다. 상기 하드웨어 복호화 장치에서 출력되는 평문은, 스마트 카드, IC(Integrated Circuit) 카드, 인터넷 통신, 무선 랜(LAN) 통신 등과 같은 시스템에서 전송되는 비빌 정보나 인증/서명 데이터이다. 복호화 과정은, 위에서 기술된 AES 암호화 과정의 역과정을 수행하는 것으로, 도 1과 같이, 하드웨어 암호화 장치(100)가 10 라운드 연산을 수행하는 경우에 상기 하드웨어 복호화 장치는 암호화 과정의 역과정을 더 수행하여 총 20 라운드 연산을 수행한다. 상기 하드웨어 복호화 장치는 합산기(1100)와 10개의 라운드(1200~1500)를 수행함으로써 평문을 출력한다. 복호화시 사용되는 키들(INKEY~KEY10)은 암호화시 사용되는 키들(INKEY~KEY10)을 역순으로 사용한다. 우선 키 스케쥴러(400)는 복호화를 위해 입력키(INKEY)를 이용하여 암호화 과정과 동일한 방법으로 KEY1부터 KEY10까지 생성한다. KEY10이 생성되면 도 10과 같은 복호화 과정을 수행하며, 이때 키 스케쥴러(400)에 의해 각각의 라운드(1200~1500)에서 사용되는 라운드 키들(KEY9~INKEY)이 생성된다. 이때 이와 같은 복호화 과정에 필요한 시스템 클럭 싸이클 수는, 위에서 기술한 바와 같이, 20 싸이클이 요구된다.

<69> 도 11은 도 10의 복호 과정에 있는 제10 라운드 내지 제2 라운드(1200~1400)를 나타내는 구체적인 블록도이다. 도 11에 도시된 바와 같이, 상기 라운드 들(1200~1400)은 역 Shift_Row 회로(1600)에서 암호문(I_INCIPH)을 "역 Shift_Row 변환"한 후, 역 Sub_Byte 회로(1700)에서 "역 Sub_Byte 변환"을 수행한다. 상기 역 Sub_Byte 회로(1700)의 결과 값은 합산기(1800)에서 해당키(KEYN)와 합산되고, 그 합산 결과 값은 역 Mix_Column 회로(1900)의 입력이 된다. 역 Mix_Column 회로(1900)는 "역 Mix_Column 변환"을 수행한다.

<70> 도 12는 도 10의 제1 라운드(1500)를 나타내는 구체적인 블록도이다. 도 12를 참조하면, 도 10의 제1 라운드(1500)는 역 Shift_Row 회로(2000), 역 Sub_Byte 회로(2100), 및 합산기(2200)를 구비한다. 최종 라운드인 상기 제1 라운드(1500)에서는, "역 Shift_Row 변환", "역 Sub_Byte 변환", 및 "Add_Round_Key 연산"으로 이루어진 라운드 연산이 1번 수행된다.

<71> 도 13은 도 11 및 도 12의 역 SUB_BYTE 회로(1700, 2100)에 사용되는 역 S-BOX를 나타내는 구체적인 블록도이다. 도 13을 참조하면, 역 S-BOX는 역 아핀 변환부(inverse affine transformation unit)(2300), 델타 변환부(δ : isomorphic transformation unit)(2400), 역원 계산부(inverse operation unit)(2500), 및 역 델타 변환

부(δ^{-1} : inverse isomorphic transformation unit)(2600)를 통하여, 도 5의 암호화 변환의 역과정을 수행한다.

<72> 이 분야에 통상의 지식을 가진 자라면, 도 10 내지 도 13의 역 변환 과정은 충분히 이해될 수 있고, 실제 하드웨어로 구현할 수 있으므로, 이러한 역 변환 과정에 대해서 구체적인 설명을 생략한다.

<73> 위에서 기술한 바와 같이, 본 발명의 일실시예에 따른 AES 방식의 하드웨어 암호화/복호화 장치에서, 비선형 변환 함수에 따른 연산을 수행하는 S-BOX(도 5)는, $GF(2^8)$ 상의 원소의 곱셈의 역원 계산(multiplicative inverse)을 합성 필드(composite field)로 이루어진 $GF(((2^2)^2)^2)$ 상의 연산을 이용하여 계산한다. 또한, 상기 하드웨어 암호화/복호화 장치는 초기 라운드 키 생성 시 클럭 낭비가 없고 각 라운드에서 사용되는 키(KEYN)를 매 클럭마다 생성하는 최적화된 키 스케쥴러(400) 구조를 적용한다. 따라서, S-BOX(도 5) 또는 역 S-BOX(도 13)의 게이트 사이즈가 약 400개 정도로 되어 하드웨어 부담을 줄일 수 있고, 종래 기술에 비하여 비선형 변환 함수 연산을 위한 클럭 수가 줄어든다. 이와 같은 S-BOX(도 5) 또는 역 S-BOX(도 13)의 연산은 가변적인 키 길이, 즉, 128, 192, 및 256 비트 각각에 따라서 10, 12, 및 14 라운드에서 수행된다.

<74> 이상에서와 같이 도면과 명세서에서 최적 실시예가 개시되었다. 여기서 특정한 용어들이 사용되었으나, 이는 단지 본 발명을 설명하기 위한 목적에서 사용된 것이지 의미한정이나 특허청구범위에 기재된 본 발명의 범위를 제한하기 위하여 사용된 것은 아니다. 그러므로 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 특허청구범위의 기술적 사상에 의해 정해져야 할 것이다.

발명의 효과

<75> 상술한 바와 같이 본 발명에 따른 하드웨어 암호화/복호화 장치는, AES 암호화 알고리즘 구현에서 S-BOX가 차지하는 하드웨어 면적과 라운드 키 발생 클럭을 최소화할 수 있다. 따라서, 작은 면적과 빠른 동작 속도가 요구되는 스마트 카드나 IC 카드 등 소형 시스템에 용이하게 적용할 수 있는 효과가 있다.

도면의 간단한 설명

<1> 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 간단한 설명이 제공된다.

<2> 도 1은 본 발명의 일실시예에 따른 하드웨어 암호화 장치의 블록도이다.

<3> 도 2는 도 1의 제1 라운드(120) 내지 제9 라운드(140)를 나타내는 구체적인 블록도이다.

<4> 도 3은 도 1의 제10 라운드(150)를 나타내는 구체적인 블록도이다.

<5> 도 4는 도 1의 키들을 발생시키는 키 스케쥴러를 나타내는 블록도이다.

<6> 도 5는 도 2 및 도 3의 Sub_Byte 회로(160)에서 사용되는 S-BOX를 나타내는 블록도이다.

<7> 도 6은 $GF(((2^2)^2)^2)$ 상에서 역원 계산을 위한 도 5의 역원 계산부(162)를 나타내는 구체적인 블록도이다.

<8> 도 7은 $GF((2^2)^2)$ 상에서 역원 계산을 위한 도 6의 제1 역원 계산기(605)를 나타내는 구체적인 블록도이다.

<9> 도 8은 $GF((2^2)^2)$ 상에서 승산을 위한 도 6의 4비트 승산기(602, 606, 607)를 나타내는 구체적인 블록도이다.

<10> 도 9는 $GF(2^2)$ 상에서 승산을 위한 도 7 및 도 8의 2비트 승산기(702, 707, 708, 803, 804, 805)를 나타내는 구체적인 블록도이다.

<11> 도 10은 도 1의 하드웨어 암호화 장치로부터 전송된 암호문을 복호하는 하드웨어 복호화 장치를 나타내는 일례이다.

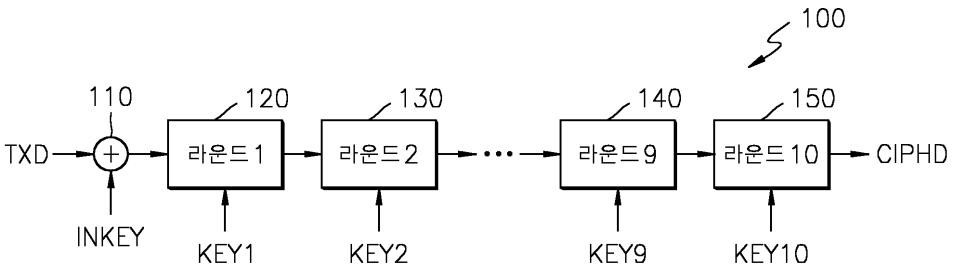
<12> 도 11은 도 10의 복호 과정에 있는 제10 라운드 내지 제2 라운드(1200~1400)를 나타내는 구체적인 블록도이다.

<13> 도 12는 도 10의 제1 라운드(1500)를 나타내는 구체적인 블록도이다.

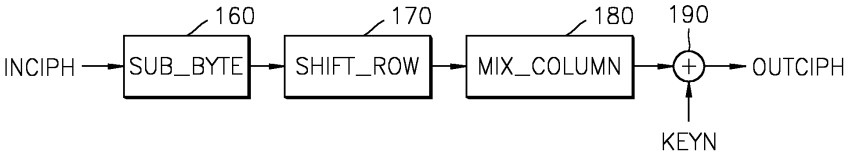
<14> 도 13은 도 11 및 도 12의 역 Sub_Byte 회로(1700, 2100)에서 사용되는 역 S-BOX를 나타내는 블록도이다.

도면

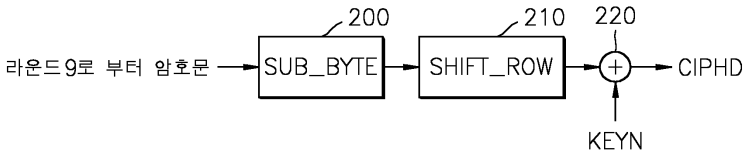
도면1



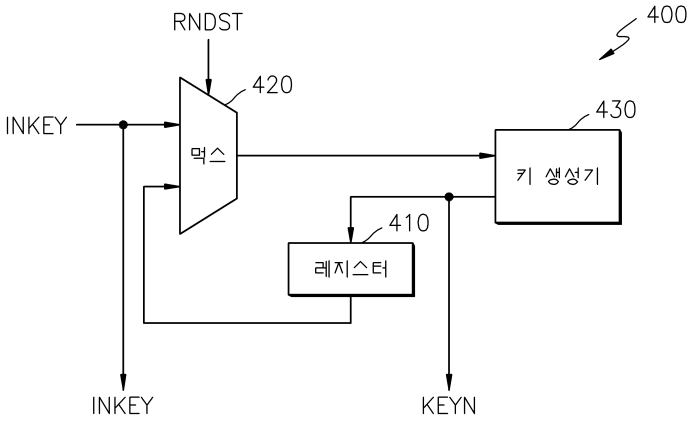
도면2



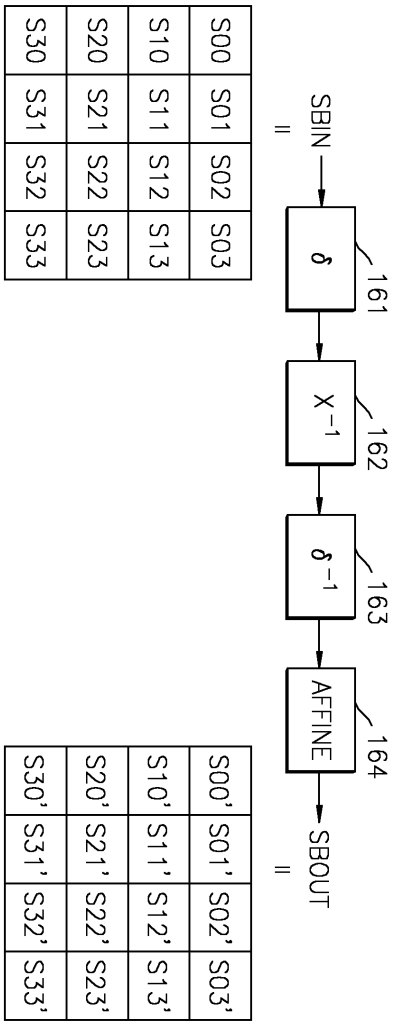
도면3



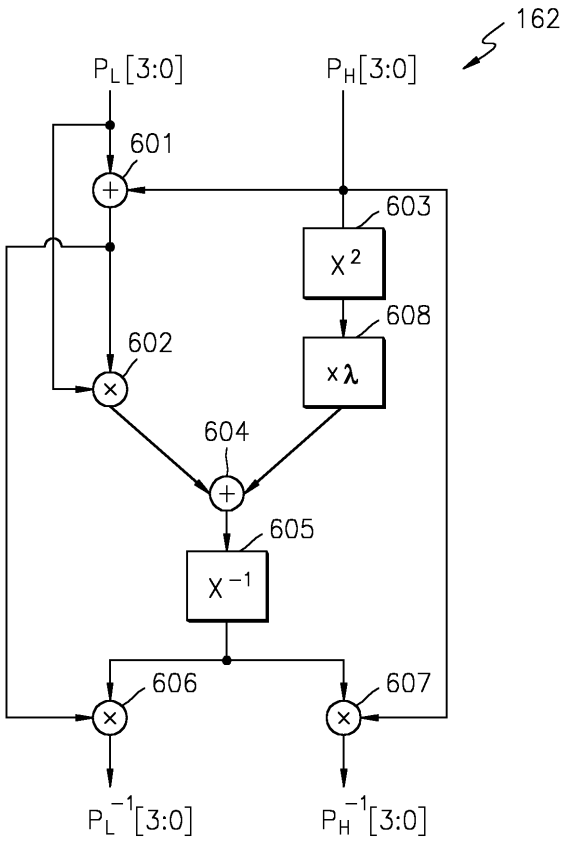
도면4



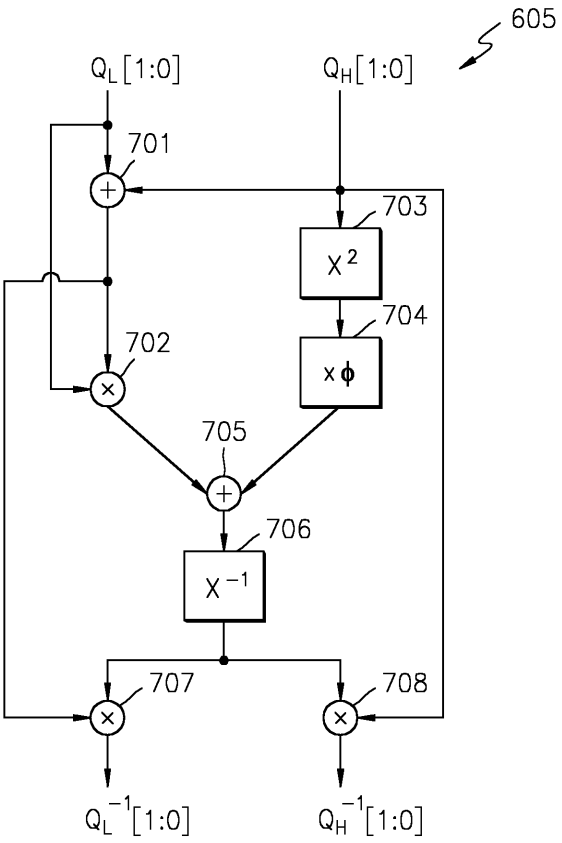
도면5


S00 S01 S02 S03
S10 S11 S12 S13
S20 S21 S22 S23
S30 S31 S32 S33
SBIN
δ
161
X⁻¹
162
δ⁻¹
163
AFFINE
164
SBOUT
S00' S01' S02' S03'
S10' S11' S12' S13'
S20' S21' S22' S23'
S30' S31' S32' S33'

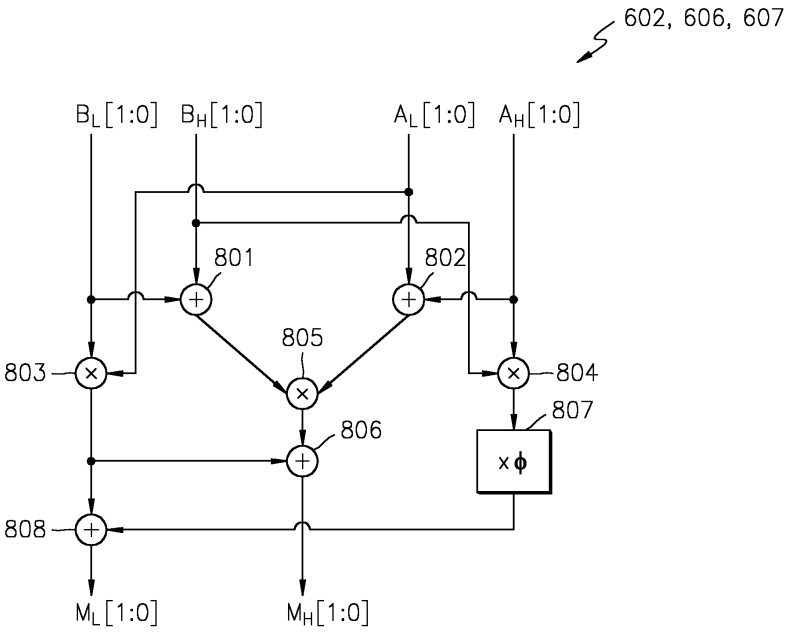
도면6


162
$P_L[3:0]$
$P_H[3:0]$
601
603
X^2
608
$x\lambda$
602
604
605
X^{-1}
606
607
$P_L^{-1}[3:0]$
$P_H^{-1}[3:0]$

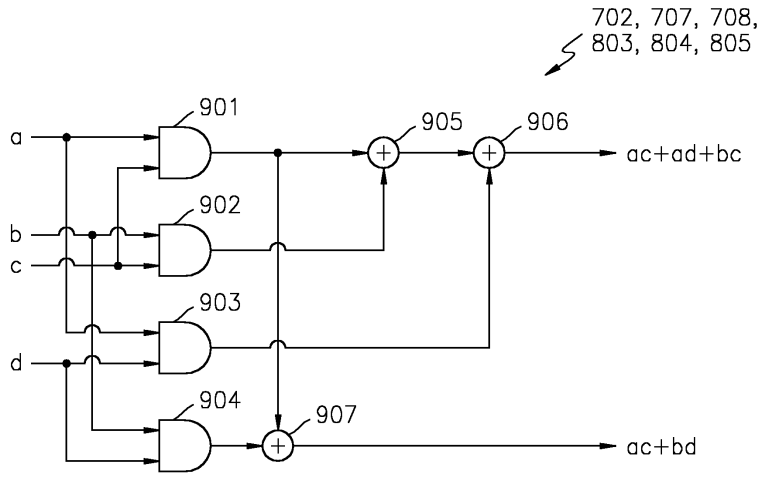
도면7


605
$Q_L[1:0]$
$Q_H[1:0]$
701
703
X^2
704
$x\phi$
702
705
706
X^{-1}
707
708
$Q_L^{-1}[1:0]$
$Q_H^{-1}[1:0]$

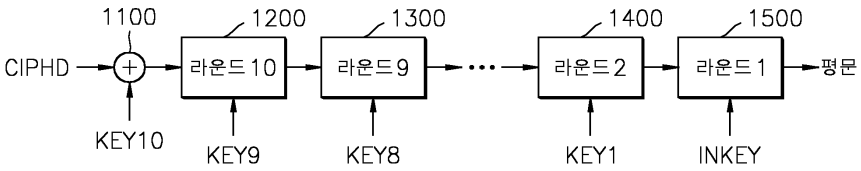
도면8


602, 606, 607
$B_L[1:0]$
$B_H[1:0]$
$A_L[1:0]$
$A_H[1:0]$
801
802
805
803
804
807
806
$x\phi$
808
$M_L[1:0]$
$M_H[1:0]$

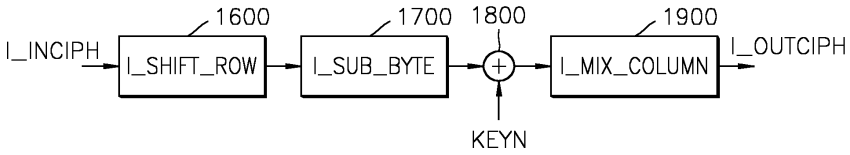
도면9



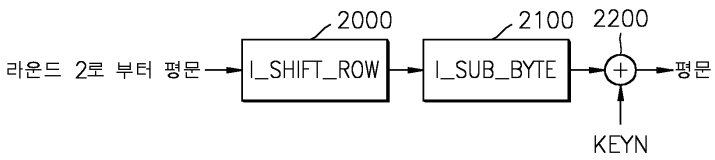
도면10



도면11



도면12



도면13