(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2021-0070075
(43) 공개일자 2021년06월14일

(51) 국제특허분류(Int. Cl.)
H04L 9/06 (2006.01) *H04L 9/08* (2006.01)
(52) CPC특허분류
H04L 9/0631 (2013.01)
H04L 9/0816 (2013.01)
(21) 출원번호 10-2019-0160101
(22) 출원일자 2019년12월04일
심사청구일자 2019년12월04일

(71) 출원인
한발대학교 산학협력단
대전광역시 유성구 동서대로 125 (덕명동)
(72) 발명자
류광기
대전광역시 유성구 동서대로 125 한밭대학교 N4동 407호
안트위 알렉산더 오우수안사
대전광역시 유성구 동서대로 125 한밭대학교 N4동 513호
(74) 대리인
특허법인 플러스

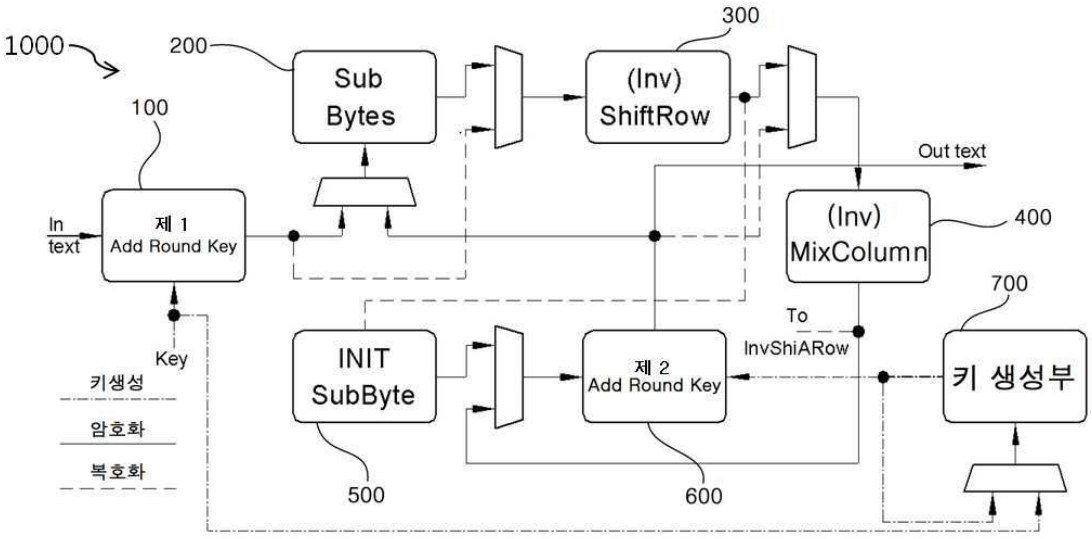
전체 청구항 수 : 총 7 항

(54) 발명의 명칭 **AES 암호화 시스템의 공유 모듈 장치**

(57) 요 약

본 발명은 AES 암호화 시스템의 공유 모듈 장치에 관한 것으로, 더욱 자세하게는 자원이 제한적인 장치에서 사용될 수 있는 AES 알고리즘의 효율적인 하드웨어를 구현하고 MixColumn/InvMixColumn 레이어에서 병렬 처리를 하여 임계 경로를 줄이고 전체 설계의 경로의 지연 시간 감소시키고 낮은 영역을 위해 단일 32 비트 XOR 게이트를 사용하여 키생성기는 암호화 및 복호화 프로세스를 위해 4 사이클마다 라운드 키를 출력하는 AES 암호화 시스템의 공유 모듈 장치에 관한 것이다.

대 표 도 - 도1



(52) CPC특허분류
H04L 9/0877 (2013.01)
H04L 2209/125 (2013.01)
H04L 2209/24 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711072771
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기술진흥센터
연구사업명	해외ICT전문인력활용촉진사업
연구과제명	사물인터넷을 위한 보안용 암호화 모듈 및 SoC 개발
기 여 율	1/1
과제수행기관명	한밭대학교산학협력단
연구기간	2018.01.01 ~ 2018.12.31

명 세 서

청구범위

청구항 1

AES 암호화 및 복호화 회로로서,

제1 AddRoundKey 변환모듈;

제2 AddRoundKey 변환모듈;

ShiftRow 변환모듈;

SubByte 변환모듈;

동작이 겹치는 레이어를 병렬로 연결하여 라운드 키를 수행하는 공유변환모듈; 및

상기 AES 암호화 및 복호화 회로에서 생성된 라운드 키를 계산하기위해 복수의 라운드 키를 계산하여 공유 키를 생성하는 키생성부를 포함하되,

하나의 주기를 기반으로 암호화와 복호화가 수행되는 것을 특징으로 하는 AES 암호화 시스템의 공유 모듈 장치.

청구항 2

제 1항에 있어서,

상기 공유변환모듈은,

MixColumn 변환모듈 및 Inverse MixColumn 변환모듈을 포함하는 것을 특징으로 하는 AES 암호화 시스템의 공유 모듈 장치.

청구항 3

제 1항에 있어서,

상기 공유변환모듈은,

ShiftRow 변환모듈 및 Inverse ShiftRow 변환모듈을 포함하는 것을 특징으로 하는 AES 암호화 시스템의 공유 모듈 장치.

청구항 4

제 2항에 있어서,

상기 공유변환모듈은,

8비트의 모듈이 4개 수행되는 것을 특징으로 하는 AES 암호화 시스템의 공유 모듈 장치.

청구항 5

제 2항에 있어서,

상기 공유변환모듈은,

0x02의 곱셈을 기반으로 수행되는 것을 특징으로 하는 AES 암호화 시스템의 공유 모듈 장치.

청구항 6

제 1항에 있어서,

상기 키생성부는,

32비트 XOR 게이트를 포함하는 것을 특징으로 하는 AES 암호화 시스템의 공유 모듈 장치.

청구항 7

제 1항에 있어서,

상기 키생성부는,

각 사이클, 단일 XOR 게이트가 상기 32비트 XOR 게이트 값을 계산하고 변속레지스터가 해당 값을 변경하는 것을 특징으로 하는 AES 암호화 시스템의 공유 모듈 장치.

발명의 설명

기 술 분 야

[0001] 본 발명은 AES 암호화 시스템에 관한 것으로, 더욱 상세하게는 AES 암호화 알고리즘에서 부분적으로 병렬 처리하여 모듈을 공유하는 것에 관한 것이다.

배 경 기 술

[0002] 현대의 무선 통신에 의한 정보 교류에 있어서 개인정보보호와 보안에 대한 요구는 IT 기술의 발전과 더불어 급격히 증가하고 있는 추세이다. 개인 정보는 인터넷을 통해 쉽게 접근할 수 있을 뿐만 아니라 널리 퍼져 있기 때문에 사물 인터넷 기술이 이용되는 장치 대 장치 또는 장치 대 인간의 관계에 있어 정보 유출에 대한 예방의 조치가 요구된다. 현재 사용되고 있는 가장 강력한 암호화 알고리즘 중의 하나는 AES(Advanced Encription Standard) 암호화 시스템이다.

[0003] AES 암호화 시스템은 표준 암호화 알고리즘으로 암호화와 복호화 과정에서 동일한 키를 사용하는 대칭 키 알고리즘을 사용하고, Rijndael 암호 알고리즘이 표준으로 사용된다. 기본적으로 128비트 단위로 이루어지고, AddRoundKey, SubByte, ShiftRow, MixColumn이 반복되어 이루어진다.

[0004] 종래에는 AES 암호화 시스템의 암호화 및 복호화에 관한 기술로서, 공개특허공보 10-2010-0029871("AES 라인달 알고리즘을 이용하는 암호화 및 복호화 장치와 그 방법", 2010.03.18., 이하 '선행문헌'이라고 함)와 같은 기술에는 AES 알고리즘을 이용한 암호화 시스템 기술이 개시되어 있다.

[0005] 선행문헌에서는 일반적인 AES 암호화 및 복호화 과정을 반복하여 수행하고 있고, 라운드키를 계산하기 위해 사용하는 8개의 XOR 모듈을 사용하기 때문에 빠르게 암호화 및 복호화를 수행할 수 있지만, 자원이 제한적인 하드웨어 장치에서 효율적인 공간 면적 사용이 불가능하다는 문제점이 야기되었다.

선행기술문헌

특허문헌

[0006] (특허문헌 0001) 공개특허공보 10-2010-0029871("AES 라인달 알고리즘을 이용한 암호화 및 복호화 장치와 그 방법", 2010.03.18.)

발명의 내용

해결하려는 과제

[0007] 본 발명은 상기와 같은 문제점을 해결하기 위하여 안출된 것으로서 본 발명의 목적은, 공유된 Mixcolumn 및 invmixcolumn 에서 병렬처리를 사용하여 임계 경로가 줄어들 수 있도록 하고, 32비트 XOR 게이트를 사용하며, 키생성기는 4 사이클마다 라운드 키를 출력할 수 있는 AES 암호화 시스템을 제공함에 있다.

과제의 해결 수단

[0008] 본 발명의 일 실시예에 따른 본 발명의 AES 암호화 시스템은 AES 암호화 및 복호화 회로로서, 제1 AddRoundKey 변환모듈; 제2 AddRoundKey 변환모듈; ShiftRow 변환모듈; SubByte 변환모듈; 동작이 겹치는 레이어를 병렬로 연결하여 라운드 키를 수행하는 공유변환모듈; 및 상기 AES 암호화 및 복호화 회로에서 생성된 라운드 키를 계산하기위해 복수의 라운드 키를 계산하여 공유 키를 생성하는 키생성부를 포함하되, 하나의 주기를 기반으로 암호화와 복호화가 수행되는 것을 특징으로 한다.

[0009] 또한, 상기 공유변환모듈은, MixColumn 변환모듈 및 InvMixColumn 변환모듈을 포함하는 것을 특징으로 한다.

[0010] 또한, 상기 공유변환모듈은, ShiftRow 변환모듈 및 Inverse ShiftRow 변환모듈을 포함하는 것을 특징으로 한다.

[0011] 또한, 상기 공유변환모듈은, 8비트의 모듈이 4개 수행되는 것을 특징으로 한다.

[0012] 또한, 상기 공유변환모듈은, 0x02의 곱셈을 기반으로 수행되는 것을 특징으로 한다.

[0013] 또한, 상기 키생성부는, 32비트 XOR 게이트를 포함하는 것을 특징으로 한다.

[0014] 또한, 상기 키생성부는, 각 사이클, 단일 XOR 게이트가 상기 32비트 XOR게이트 값을 계산하고 변속레지스터가 해당 값을 변경하는 것을 특징으로 한다.,

발명의 효과

[0015] 상기와 같은 구성에 의한 본 발명의 AES 암호화 시스템은 4단계의 하위 파이프라인 암호화 및 복호화 설계에 따라 공유된 MixColumn/InvMixColumn 레이어에서 병렬 처리를 사용하면 임계 경로가 줄어들어 전체 경로에서 지연시간이 감소할 수 있다는 효과가 있다.

[0016] 또한, 본 발명에 따르면, 단일 32비트 XOR이 사용되어 4사이클마다 라운드키를 출력할 수 있다는 효과가 있다.

도면의 간단한 설명

[0017] 도 1은 본 발명의 일 실시예에 따른 AES 암호화 시스템의 공유 모듈 장치의 개념도이다.

도 2는 본 발명의 일 실시예에 따른 AES 암호화 시스템의 공유 모듈 장치의 MixColumn 및 InvMixColumn 모듈 회로 구성도이다.

도 3은 본 발명의 일 실시예에 따른 공통변환모듈의 공통 단위 회로 구성도이다.

도 4는 본 발명의 일 실시예에 따른 AES 암호화 시스템의 공유 모듈 장치의 공통 단위 회로의 Mult_02 유닛의 구성도이다.

도 5는 본 발명의 일 실시예에 따른 AES 암호화 시스템의 공유 모듈 장치의 키생성부의 구성도이다.

발명을 실시하기 위한 구체적인 내용

[0018] 이하, 본 발명의 기술적 사상을 첨부된 도면을 사용하여 더욱 구체적으로 설명한다. 이에 앞서, 본 명세서 및 청구범위에 사용된 용어나 단어는 통상적이거나 사전적인 의미로 한정해서 해석되어서는 아니되며, 발명자는 그 자신의 발명을 가장 최선의 방법으로 설명하기 위해 용어의 개념을 적절하게 정의할 수 있다는 원칙에 입각하여 본 발명의 기술적 사상에 부합하는 의미와 개념으로 해석되어야만 한다.

[0019] 따라서, 본 명세서에 기재된 실시예와 도면에 도시된 구성은 본 발명의 가장 바람직한 일 실시예에 불과할 뿐이고 본 발명의 기술적 사상을 모두 대변하는 것은 아니므로, 본 출원시점에 있어서 이들을 대체할 수 있는 다양한 변형 예들이 있을 수 있음을 이해하여야 한다.

[0020] 이하, 본 발명의 기술적 사상을 첨부된 도면을 사용하여 더욱 구체적으로 설명한다. 첨부된 도면은 본 발명의 기술적 사상을 더욱 구체적으로 설명하기 위하여 도시한 일예에 불과하므로 본 발명의 기술적 사상이 첨부된 도

면의 형태에 한정되는 것은 아니다.

[0021] 도 1은 본 발명의 일 실시예에 따른 AES 암호화 시스템의 개념도를 도시하는 것이다. 도 1에 도시된 바와 같이 본 발명의 일 실시예에 따른 AES 암호화 시스템은, 기본적으로 제 1 Add Round Key 변환모듈(100), SubBytes 변환모듈(200), ShiftRow 변환모듈(300), MixColumn 변환모듈(400), INITSubBytes 변환모듈(500), 제 2 Add Round Key 변환모듈(600)을 포함하여 구성되고, 4단계의 파이프라인의 설계로 암호화 및 복호화된다. 파이프라인은 라운드키 변환을 주기별로 수행하고, 모든 주기에서 계산된 각 변환은 각각의 레지스터에 저장된다. 각각의 레지스터에 저장된 값은 다음 라운드키 변환의 계산에 사용된다.

[0022] 도 1을 참조하면, 암호화를 하는 과정은 제 1 Add Round Key 변환모듈(100), SubBytes 변환모듈(200), ShiftRow 변환모듈(300), MixColumn 변환모듈(400), 제 2 Add Round Key 변환모듈(600), SubBytes 변환모듈(200)의 순서로 암호화를 수행하고, 복호화를 하는 과정은 제 1 Add Round Key 변환모듈(100), INITSubBytes 변환모듈(500), 제 2 Add Round Key 변환모듈(600), InvMixColumn 변환모듈(400), InvShiftRow(300)의 순서로 복호화를 수행한다.

[0023] 일반적으로, AES 암호알고리즘은 하나의 라운드 동작이 SubBytes 변환모듈(200), ShiftRow 변환모듈(300), MixColumn 변환모듈(400), Add Round Key(100, 600) 동작으로 구성되는데, 각각의 부분 라운드는 하드웨어 공유를 위해 4클록으로 구현하고, 동작 속도 개선을 위해 현재 라운드의 후반부 부분 라운드와 다음 라운드의 전반부 부분 라운드 간에 파이프라인이 적용되는 기법을 적용한다. 여기서, 전반부 부분 라운드는 SubBytes 변환모듈(200)과 ShiftRow 변환모듈(300)의 동작을 구현하며, MixColumn 변환모듈(400)과 제 2 Add Round Key 변환모듈(600)은 후반부 부분 라운드 동작을 구성한다. 첫 번째 라운드는 입력부에 제 1 AddRoundKey(100) 동작이 추가되고 마지막 라운드는 기존 라운드 동작에 비해 MixColumn 변환모듈(400)의 동작이 없는 동작 특성을 갖는다.

[0024] 암호화의 경우, 라운드키의 출력 사이클과 일치하는 파이프라인의 네 번째 사이클에서 제 2 AddRoundKey(600)가 수행되고, 복호화의 경우, 파이프라인의 세 번째 사이클에서 제 2 AddRoundKey(600)가 수행된다.

[0025] 여기서, 도 1을 참조하면, ShiftRow 변환모듈(300) 및 InvShiftRow 변환모듈(300)를 병렬 처리하여 레이어를 서로 공유하고 MixColumn 변환모듈(400) 및 InvMixColumn 변환모듈(400)을 병렬 처리하여 레이어를 서로 공유하도록 설계되었다. 여기서, 병렬 처리된 레이어들을 공유변환모듈이라고 한다. 상기 공유변환모듈은 레이어를 공유해서 사용하면서, 각각의 공유 모듈을 설계하는 과정에서 전선을 재배치해 각각의 모듈을 공유하도록 설계하기 때문에 추가적인 비용이 들지 않아도 하드웨어의 면적을 최적화시킬 수 있다는 효과가 있고, 작은 면적에서도 AES 알고리즘의 높은 처리량을 나타낼 수 있는 장점이 있으며, 임계경로가 줄어들어 전체 설계 경로의 지연 시간이 감소된다는 효과가 있다. 더 자세하게 설명하자면, ShiftRow 변환을 위해 각 비트의 수를 왼쪽으로 쉬프트하는 것이 바람직하고 InvShiftRow 변환을 위해 주기적으로 각 비트의 수를 쉬프트하는 것이 바람직하다.

[0026] 도 2는 본 발명의 일 실시예에 따른 AES 암호화 시스템의 MixColumn 및 InvMixColumn 모듈 회로 구성도를 나타낸 도면이다. 도 2에 도시된 바와 같이 본 발명의 일 실시예에 따른 AES 암호화 시스템의 MixColumn 및 InvMixColumn 변환모듈의 암호화 및 복호화를 도 2의 (a)와 도 2의 (b)를 통해 자세하게 설명한다.

[0027] MixColumn 변환모듈(400) 및 InvMixColumn 변환모듈(400)은 32비트로 작동하고 총 4개의 모듈이 동시에 작동된다. 도 2의 (a)는 MixColumn 변환모듈(400) 및 InvMixColumn 변환모듈(400)에서 MixColumn 변환모듈(400)에서 암호화하는 것을 나타낸 것이고, MixColumn 변환모듈(400)의 변환은 ShiftRow 변환모듈(300) 변환 후 수행되는 것이 바람직하다.

[0028] 도 2의 (b)는 MixColumn 및 InvMixColumn 모듈에서 InvMixColumn에서 복호화하는 것을 나타낸 것이고, InvMixColumn 변환모듈(400)은 제 2 AddRoundKey(600) 변환 후 수행되는 것이 바람직하다. 암호화의 마지막 라운드와 암호 해독의 첫 번째 라운드의 경우, 역연산이나 비트의 이동이 없다.

[0029] 도 2의 (a) 및 (b)를 참조하면, 단일 MixColumn 변환모듈(400)은 단일 열에서 수행되고, 모듈 4개를 중복해서 수행되기 때문에 낮은 임계 경로에서 사용될 수 있다. 4바이트 입력의 각 바이트는 암호화의 경우 0x01, 0x02, 0x03의 요소를 곱하고 복호화의 경우 0x09, 0x0B, 0x0E의 요소를 곱한다. 출력 바이트를 제공하기 위해 XOR로 연결되고, 공유 모듈은 4바이트로 출력되기 위해 동시에 입력을 하는 것이 바람직하다.

[0030] 도 3은 본 발명의 일 실시예에 따른 AES 암호화 시스템의 공유변환모듈의 공통 단위 회로 구성도이고, 도 4는 본 발명의 일 실시예에 따른 AES 암호화 시스템의 공통 단위 회로의 Mult_02 유닛의 구성도를 나타낸 도면이다. 도 3과 도 4에 도시된 바와 같이 본 발명의 일 실시예에 따른 AES 암호화 시스템의 공유변환모듈과 Mult_02를

설명한다.

[0031] 도 3과 도 4를 참조하면, 상기 Mult_02는 ShiftRow 변환모듈(300) 및 InvShiftRow 변환모듈(300), MixColumn 변환모듈(400) 및 Inv MixColumn 변환모듈(400)의 공유변환모듈의 공통된 기본 단위이고, 02에 의한 곱셈의 경우 첫 번째 Mult_02 모듈에서 출력되는 것이 바람직하고, 04 또는 08에 의한 곱셈의 경우 두 번째 Mult_02 모듈 또는 세 번째 Mult_02 모듈에서 출력하는 것이 바람직하다. 더불어, Mult_02 유닛은 갈루아 필드를 이용하여 수행된다. 이에 따라, 본 발명의 Mult_02 유닛은 기본적으로 좌측 시프트와 조건부 XOR를 사용하고, 3개의 2비트 XOR 게이트를 사용해서 0x02 곱셈을 수행한다. 더 자세하게 설명하자면, 하나의 실시예로, A를 0B로 곱하기 위해서 0x09와 0x02를 사용하는 대신에 0x08,0x02 및 0x01의 조합을 사용하게 된다. 이에 따라, 본 발명의 회로는 전체 회로의 게이트 카운트와 임계 경로를 줄일 수 있다는 장점이 있다.

[0032] 도 5는 본 발명의 일 실시예에 따른 AES 암호화 시스템의 키생성부의 구성도를 나타낸 도면이다. 도 5에 도시된 바와 같이 AES 암호화 시스템의 키생성부는 낮은 영역을 유지하기 위해 메모리 장치의 공간 면적 사용을 줄이고 있다. 키생성부는 초기 키값을 가지고 각 라운드의 하위 키 값을 계산한다.

[0033] 도 5를 참조하면, 키생성부는 AES 암호화 및 복호화 장치의 과정을 수행하면서 생성된 라운드 키를 계산하기 위해 복수의 라운드 키를 계산하여 공유키를 생성한다. 상기 키생성부는 하나의 32비트 XOR, 8 deep Shift Register, SRRC 모듈, 카운터 유닛, 스위치 유닛 및 라운드 컨스턴트로 구성된다.

[0034] 상기 8 deep Shift Register는 하위키와 출력 라우팅을 수행하는 역할을 한다.

[0035] 상기 SRRC 모듈은 S-BOX, ROTWORD, ADDROUNDCONSTANT(S-BOX 연산, ROTWORD 연산, ADDRONDCONSTANT 연산)를 포함하여 구성된다. 상기 S-BOX(Substitution Box)는 도 1에서 설명한 바와 같이 암호화 및 복호화를 수행하는 부분으로, 공지되어 있는 S-BOX 생성 알고리즘을 이용하여 생성되는, Byte 값의 대체를 수행하기 위해 Key Expansion Routine과 여러 SubBytes 변환에서 사용되는 비선형 대칭표로서, SubBytes 단계에서 각 바이트마다 S-BOX 테이블 표를 이용하여 치환하게 된다.

[0036] 상기 ROTWORD는 AES 암호화 시스템에서, Word 단위의 한 행에 대해 1회의 Left Rotation을 의미하며, 상기 ADDROUNDCONSTANT는 state 내에 각각의 byte들이 각 RoundKey와 XOR 연산되는 것을 의미하며, RoundKey는 key expansion schedule에 따라 key로부터 유도되어진다.

[0037] 각 사이클과 단일 XOR 게이트가 XOR 값을 계산하고 변속 레지스터는 각 키 모드에 따라 다르게 형성되어 해당 값을 변경한다.

[0038] 상기 32비트 XOR 게이트는 키생성 알고리즘에서 수행할 모든 XOR 게이트 작동을 계산하고, 매 4사이클마다 한 라운드씩 수행된다. 여기서, 본 발명에서 생성되는 키는 공유 키인 것이 바람직하다. 이에 따라, 상기 키생성부는 각 사이클에서 32비트의 라운드 키를 생성할 여유가 생기고, 키 생성에서 사이클 당 32비트의 데이터를 생성하기 때문에 32비트 XOR 게이트 하나만 사용할 수 있다. XOR 게이트의 출력은 Shift Register에 공급되고, 상기 Shift Resgister는 네 번의 사이클이 끝날 때 정확한 출력을 얻기 위해 매회 이동되는 8개의 32비트 레지스터로 구성된다. 출력은 시프트 레지스터 체인의 하단 32비트 레지스터에도 저장된다. 상기 키생성부에 XOR 게이트에 대한 입력이 고정되어 있기 때문에 이동 작업에서 데이터 흐름을 추적하기 위해 카운터 및 곱셈기가 필요하지 않기 때문에 하드웨어 설계 면적을 넓힐 수 있다는 효과가 있다.

[0039] Shift Register 체인의 32비트 레지스터 각각에는 시작 및 종료 신호의 AND 게이트와 시작을 설정하는 P 가 포함되어 있어, 시작 신호를 보내기 전의 초기 사이클에서 키가 변속 레지스터에 복사된다. 모든 새로운 공유 키 입력에 대해 공유 키 생성을 시작하기 전에 공유 키는 Shift Register에 복사된다.

[0040] 즉, 다시 말하자면, 본 발명의 일실시예에 따른 AES 암호화 시스템의 공유 모듈 장치는 라운드 키를 계산하기 위해 단일 XOR 게이트를 사용하는 소형 키 생성기 모듈을 특징으로 하고, AES 알고리즘의 높은 처리량과 작은 면적 구현 방법을 제공하는 것을 특징으로 한다. 본 발명의 AES 설계는 즉석 키 생성 체계 뿐만 아니라 SubBytes 변환모듈/InvSubByte 변환모듈(200)계층의 LUT 기반 구현을 사용하는 4단계 하위 파이프라인 암호화 및 복호화 설계에 관한 것이다. 공유된 MixColumn/InvMixColumn 레이어에서 병렬 처리를 사용하면 임계 경로가 줄어들어 전체 설계 경로의 지연 시간 감소에 탁월한 효과를 낼 수 있다. 본 발명은 낮은 영역 요구 사항에 따라 키 생성기를 구현할 때 단일 32비트 XOR 게이트를 포함하고, 상기 키 생성기는 암호화 및 복호화 과정을 위해 4 사이클마다 라운드 키를 출력한다. 이에 따라, 본 발명의 AES 암호화 시스템의 공유 모듈 장치는 하드웨어의 최소 면적을 사용하면서도 높은 처리량을 제공할 수 있다는 효과가 있다.

[0041] 이상과 같이 본 발명에서는 구체적인 구성 소자 등과 같은 특정 사항들과 한정된 실시예 도면에 의해 설명되었으나 이는 본 발명의 보다 전반적인 이해를 돕기 위해서 제공된 것 일 뿐, 본 발명은 상기의 일 실시예에 한정되는 것이 아니며, 본 발명이 속하는 분야에서 통상의 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다.

[0042] 따라서, 본 발명의 사상은 설명된 실시예에 국한되어 정해져서는 아니 되며, 후술하는 특허 청구 범위뿐 아니라 이 특허 청구 범위와 균등하거나 등가적 변형이 있는 모든 것들은 본 발명 사상의 범주에 속한다고 할 것이다.

부호의 설명

[0043] 1000 : AES 암호화 시스템

100 : 제 1 Add Round Key 변환모듈

200 : SubBytes 변환모듈

300 : (Inv)ShiftRow 변환모듈

400 : (Inv)MixColumn 변환모듈

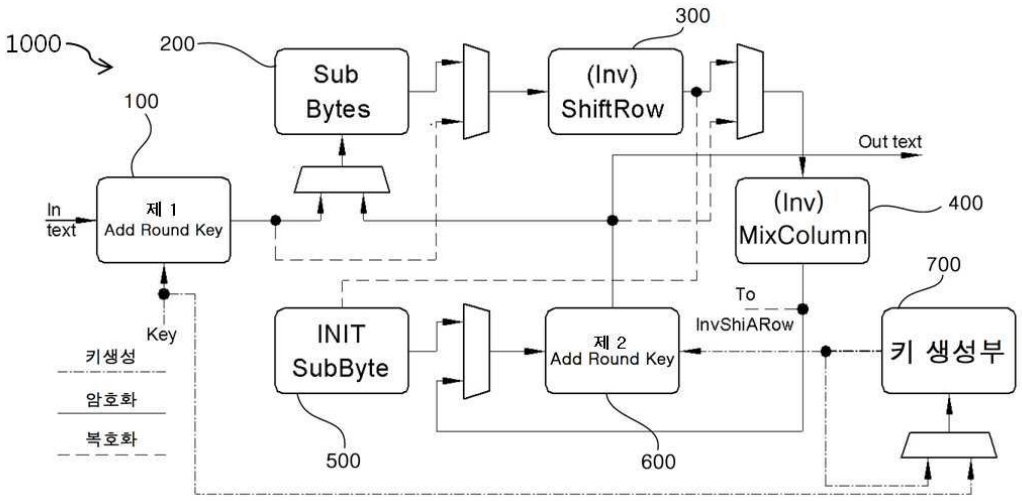
500 : INIT SubBytes 변환모듈

600 : 제 2 Add Round Key 변환모듈

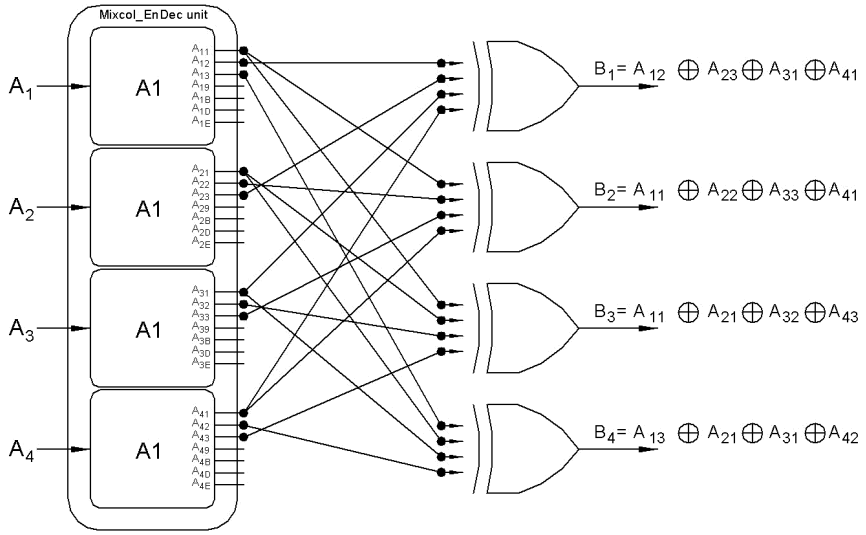
700 : 키 생성부

도면

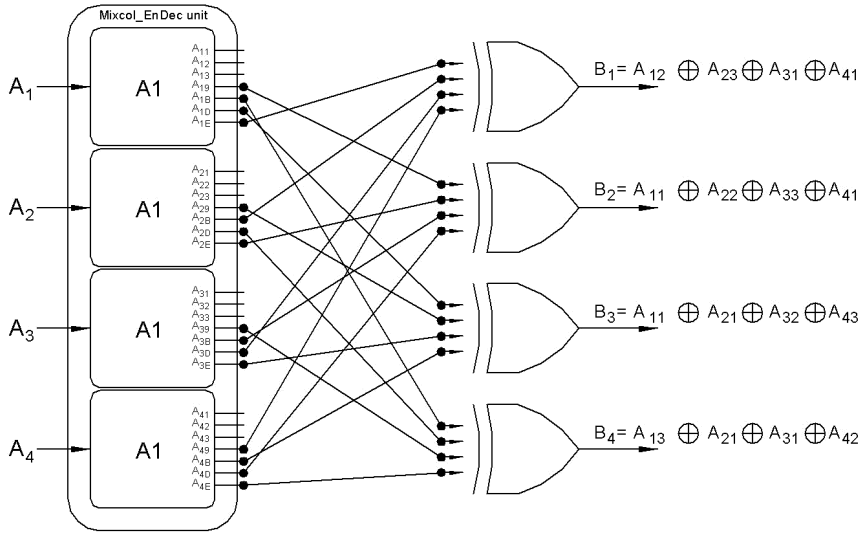
도면1



도면2

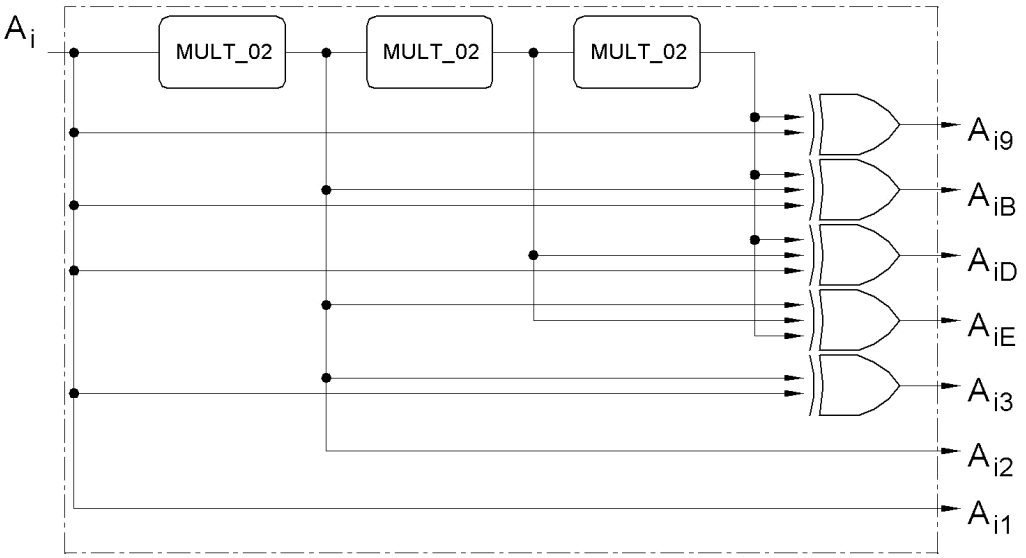

Mixcol_EnDec unit
A1
A1
A1
A1
A1
A2
A3
A4
B1= A12 ⊕ A23 ⊕ A31 ⊕A41
B2= A11 ⊕ A22 ⊕ A33 ⊕A41
B3= A11 ⊕ A21 ⊕ A32 ⊕A43
B4= A13 ⊕ A21 ⊕ A31 ⊕A42

(a)

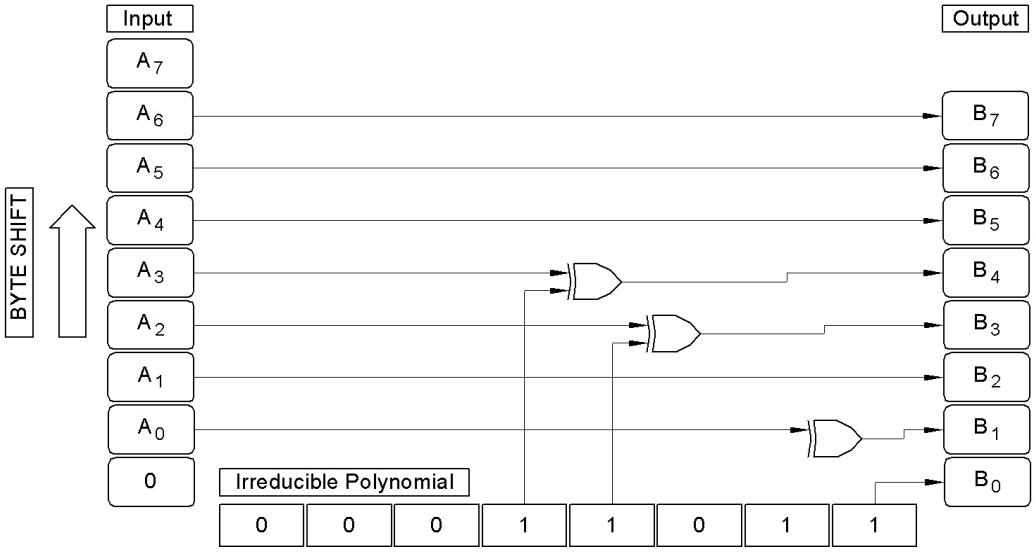

Mixcol_EnDec unit
A1
A1
A1
A1
A1
A2
A3
A4
B1= A12 ⊕ A23 ⊕ A31 ⊕A41
B2= A11 ⊕ A22 ⊕ A33 ⊕A41
B3= A11 ⊕ A21 ⊕ A32 ⊕A43
B4= A13 ⊕ A21 ⊕ A31 ⊕A42

(b)

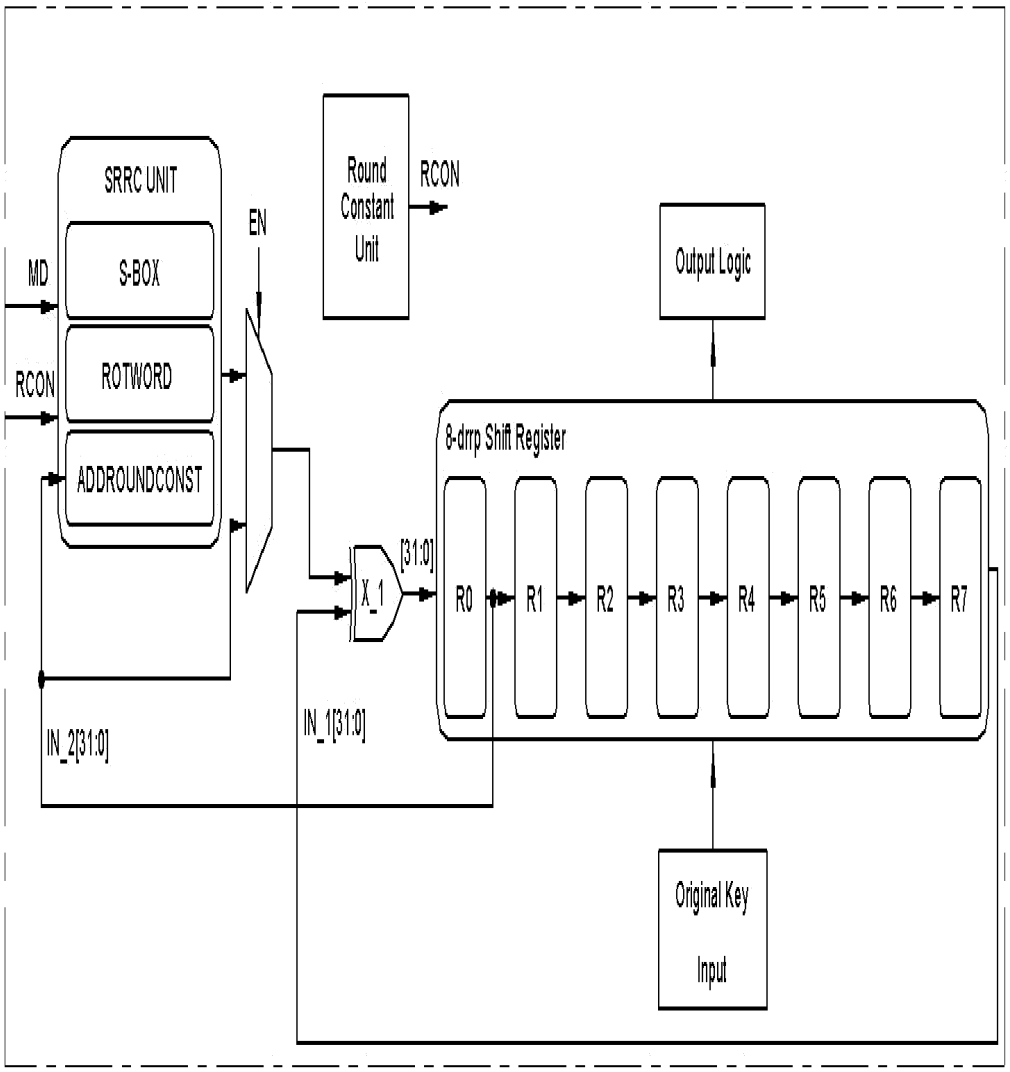
도면3


Ai
MULT_02
MULT_02
MULT_02
Ai9
AiB
AiD
AiE
Ai3
Ai2
Ai1

도면4


Input
Output
A7
A6
A5
A4
A3
A2
A1
A0
0
B7
B6
B5
B4
B3
B2
B1
B0
BYTE SHIFT
Irreducible Polynomial
0 0 0 1 1 0 1 1

도면5


SRRC UNIT
S-BOX
ROTWORD
ADDROUNDCONST
MD
RCON
EN
Round Constant Unit
RCON
Output Logic
8-drrp Shift Register
R0
R1
R2
R3
R4
R5
R6
R7
X_1
[31:0]
IN_2[31:0]
IN_1[31:0]
Original Key Input