



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2019-0037980
(43) 공개일자 2019년04월08일

(51) 국제특허분류(Int. Cl.)

H04L 9/06 (2006.01)

(52) CPC특허분류

H04L 9/0625 (2013.01)

H04L 9/0631 (2013.01)

(21) 출원번호 10-2017-0127877

(22) 출원일자 2017년09월29일

심사청구일자 2017년09월29일

(71) 출원인

한밭대학교 산학협력단

대전광역시 유성구 동서대로 125 (덕명동)

(72) 발명자

류광기

대전광역시 유성구 덕명동 한밭대학교 N4동 407호

구기 데니스

대전광역시 유성구 덕명동 한밭대학교 N4동 513호

(74) 대리인

추혁

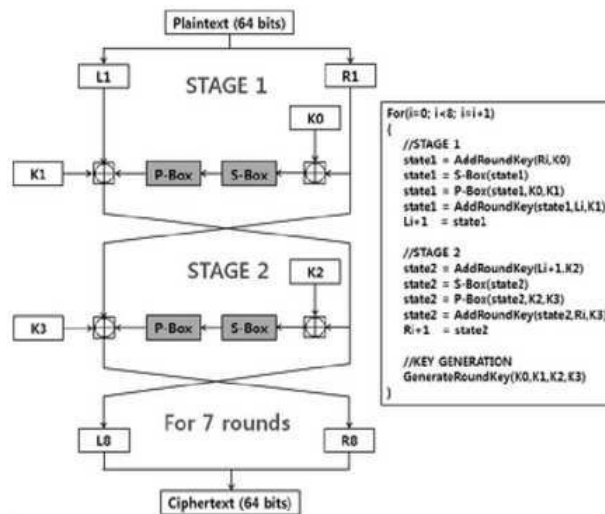
전체 청구항 수 : 총 5 항

(54) 발명의 명칭 퍼베이션 컴퓨팅을 위한 효과적인 초경량 블록 암호 시스템

(57) 요약

본 발명은 퍼베이션 컴퓨팅을 위한 효과적인 초경량 블록 암호 시스템에 관한 것으로서, 백도어 아이디어가 암호화 알고리즘에 사용되는 것을 방지하기 위한 치환-박스(Substitution-box, S-박스) 및 엄격한 애벌란시 기준 (Strict Avalanche Criterion)을 충족할 뿐만 아니라 암호 복호화를 더 어렵게 만들도록 설계된 키-의존 원 스테이지 오메가 네트워크를 사용하는 순열-박스(Permutation-box, P-박스)와 함께, 암호화 및 복호화 시 하나의 코어 실행을 가능하게 하는 파이스텔 구조를 사용함으로써, 작은 하드웨어 면적을 가지면서도 높은 처리량 암호화 알고리즘을 요구하는 퍼베이션 컴퓨팅에 매우 적합한 초경량 블록 암호를 제공한다.

대표도 - 도1



(52) CPC특허분류

H04L 2209/122 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 R01341610190001002

부처명 미래창조과학부

연구관리전문기관 정보통신기술진흥센터

연구사업명 해외 ICT 전문인력 활용 촉진사업

연구과제명 Core-A 기반 영상처리 SoC 플랫폼 개발

기 여 율 1/1

주관기관 연구사업관리팀

연구기간 2016.01.01 ~ 2016.12.31

명세서

청구범위

청구항 1

백도어 아이디어가 암호화 알고리즘에 사용되는 것을 방지하기 위한 치환-박스(Substitution-box, S-박스) 및 엄격한 애벌란시 기준(Strict Avalanche Criterion)을 충족할 뿐만 아니라 암호 복호화를 더 어렵게 만들도록 설계된 키-의존 원 스테이지 오메가 네트워크를 사용하는 순열-박스(Permutation-box, P-박스)와 함께, 암호화 및 복호화 시 하나의 코어 실행을 가능하게 하는 파이스텔 구조를 사용하는, 초경량 블록 암호 시스템.

청구항 2

청구항 1에 있어서,

64 비트 사용자 입력 데이터 및 128 비트 사용자 입력 키를 취하고, 각 라운드가 새로운 라운드 키를 사용하는 8개의 라운드로 이루어지고, 상기 각 라운드는 두 개의 스테이지로 이루어지며, 상기 두 개의 스테이지의 각각은 다음 연산: 제1 AddRoundKey, S-박스, P-박스 및 제2 AddRoundKey을 통해 데이터를 전달하는, 초경량 블록 암호 시스템.

청구항 3

청구항 2에 있어서,

상기 AddRoundKey 레이어는 상기 128 비트 사용자 입력 키를 위해 상기 8개의 라운드의 각 라운드마다 고유한 128 비트 라운드 키를 생성하고, 상기 라운드 키를 32 비트로 이루어지는 네 개의 키로 나누어 상기 두 개의 스테이지의 각각이 각각 두 개의 키를 사용하도록 구성되고,

상기 S-박스 레이어는 상기 사용자 입력 데이터의 입력 비트들의 치환을 수행함으로써 입력의 변환된 값을 나타내는 출력 비트들의 값을 갖는 출력 비트에 맵핑하도록 구성되며,

상기 P-박스 레이어는 상기 S-박스 레이어의 출력 비트들을 입력으로서 사용하는 32 대 1 다중화기들로 이루어지고, 16 비트 가변 키가 상기 다중화기들에 대한 선택 신호로서의 역할을 하며, 두 개의 다중화기가 상기 16 비트 가변 키로부터의 하나의 선택 신호에 의해 제어되도록 구성되는, 초경량 블록 암호 시스템.

청구항 4

청구항 3에 있어서,

상기 AddRoundKey 레이어는 먼저 상기 사용자 입력 키를 라운드 1의 라운드 키로 생성하고, 그 다음 라운드 i (여기서, $i=1, 2, \dots, 8$)의 라운드 키를 직전 라운드 $i-1$ 의 직전 라운드 키를 25 비트만큼 순환 시프트시켜 각 라운드에 대해 고유한 상기 라운드 키들을 생성하는, 초경량 블록 암호 시스템.

청구항 5

청구항 3에 있어서,

상기 P-박스 레이어는 상기 각 스테이지에 대해 상기 라운드 키의 절반을 사용하여 배타적-or 연산함으로써 상기 16 비트 가변 키를 생성하는, 초경량 블록 암호 시스템.

발명의 설명

기술 분야

[0001]

본 발명은 블록 암호 시스템에 관한 것으로, 더욱 상세하게는 S-박스 및 키-의존 P-박스와 함께 파이스텔 구조를 사용하는 퍼베이션 컴퓨팅을 위한 효과적인 초경량 블록 암호 시스템에 관한 것이다.

배경 기술

[0002] 오늘날 퍼베이시브 컴퓨팅의 대량 배포가 증가하고 있다. 퍼베이시브 컴퓨팅에서, 연산 능력을 갖는 디바이스들이 가전 제품들에 장착된다. 이러한 디바이스들은 그것들이 장착되는 매체에 대한 민감한 정보를 기록, 저장 및 업데이트한다. 이와 같이 퍼베이시브 디바이스들에서 이용가능한 정보가 민감하지만, 공격자들의 홈 네트워크를 통한 정보 수집 등과 같은 문제들로부터 그러한 정보를 보호하기 위한 많은 연구가 이루어지지 않았었다.

[0003] 퍼베이시브 컴퓨팅의 대량 배포의 소비 전력, 공간 및 비용의 제약으로 인해, 컴퓨팅 능력, 메모리 용량 및 전원 공급 측면에서 제약을 갖는 디바이스들을 사용하는 것이 내재한다. 퍼베이시브 컴퓨팅에서 널리 사용되는 하나의 기술은 RFID 기술이다. RFID 태그들은 약 512 비트의 사용자 메모리 용량을 갖고, 또한 응답 시간이 ISO/IEC 18000 vwnsdp 따라 $100\mu s$ 보다 짧아야 한다. 이러한 제약들로 인해, AES와 같은 표준 암호 알고리즘들이 상기한 디바이스들 상에서 구현될 수 없다. 따라서 연구의 초점은 가능한 적은 메모리를 요구하는 경량 암호화로 옮겨갔다.

[0004] 경량 암호화에 관한 ISO/IEC 표준에 따라, LUT(Look Up Table)들의 조각들의 수는 100개 내지 300개이어야 한다. ISO/IEC 표준으로 인정되었던 전혀 새로운 설계는 PRESENT 알고리즘이다. PRESENT는 이용가능한 최소한의 S-박스(S-box)들 중 하나를 갖는다. PRESENT 알고리즘은 100KHz로 블록당 $310\mu s$ 로 변환하는 데이터의 블록을 암호화하기 위해 31개의 라운드를 필요로 한다는 단점이 있다. 이는 RFID 태그들에 대한 응답 시간에 미달된다. 다른 ISO/IEC 표준 알고리즘은 SONY에 의해 개발된 CLEFIA이다. 이는 두 개의 S-박스 및 두 개의 P-박스를 사용하고 그에 따라 PRESENT 알고리즘보다 훨씬 더 많은 메모리를 필요로 한다. 표 1은 현존하는 몇몇 암호 알고리즘을 요약한다.

표 1

[0005]

알고리즘	S-박스 메모리 요건 (비트)	블록당 사이클	1 암호화 시간 @100 KHz(μs)
AES	2048	12	120
PRESENT	64	31	310
TEA	-	64	640
CLEFIA	4096	18	180
DESL	256	16	160
HIGHT	-	32	320

[0006] 따라서, 본 명세서는 새로운 경량 블록 암호의 설계 및 구현에 초점을 두고 치환-순열(S-P) 네트워크와 파이스텔 구조의 장단점을 연구하여, 두 가지 네트워크의 이용시 가장 적합한 방향을 제시한다. 이에 따라 본 발명의 목적은 RFID 태그들에 대해 $100\mu s$ 미만 응답 시간의 ISO/IEC 18000 표준 및 경량 암호들에 대해 100개 내지 300개 LUT의 ISO/IEC 표준 양자의 요건을 만족하는 새로운 경량 블록 암호의 하드웨어 설계 및 구현을 설명하는 것이다.

선행기술문헌

특허문헌

[0007]

(특허문헌 0001) 대한민국 등록특허공보 제10-1135058호(2012.04.13)

(특허문헌 0002) 대한민국 등록특허공보 제10-1593169호(2016.02.15)

(특허문헌 0003) 대한민국 등록특허공보 제10-1091749호(2011.12.08)

발명의 내용

해결하려는 과제

[0008]

따라서, 본 발명은 상기한 종래 기술의 문제점을 해결하기 위해 이루어진 것으로서, 본 발명의 목적은 백도어 아이디어가 암호화 알고리즘에 사용되는 것을 방지하기 위한 S-박스 및 엄격한 애벌란시 기준(Strict Avalanche Criterion)을 충족할 뿐만 아니라 암호 복호화를 더 어렵게 만들도록 설계된 키-의존 원 스테이지 오메가 네트워크를 사용하여 보안 단계를 향상한 P-박스와 함께, 암호화 및 복호화 시 하나의 코어 실행을 가능하게 하는

파이스텔 구조를 사용함으로써 퍼베이션 컴퓨팅을 위한 효과적인 초경량 블록 암호 시스템을 제공하는데 있다.

과제의 해결 수단

- [0009] 상기와 같은 목적을 달성하기 위한 본 발명의 퍼베이션 컴퓨팅을 위한 효과적인 초경량 블록 암호 시스템은, 백도어 아이디어가 암호화 알고리즘에 사용되는 것을 방지하기 위한 치환-박스(Substitution-box, S-박스) 및 엄격한 애벌란시 기준(Strict Avalanche Criterion)을 충족할 뿐만 아니라 암호 복호화를 더 어렵게 만들도록 설계된 키-의존 원 스테이지 오메가 네트워크를 사용하는 순열-박스(Permutation-box, P-박스)와 함께, 암호화 및 복호화 시 하나의 코어 실행을 가능하게 하는 파이스텔 구조를 사용한다.
- [0010] 바람직하게는, 상기 초경량 블록 암호 시스템은 64 비트 사용자 입력 데이터 및 128 비트 사용자 입력 키를 취하고, 각 라운드가 새로운 라운드 키를 사용하는 8개의 라운드로 이루어지고, 상기 각 라운드는 두 개의 스테이지로 이루어지며, 상기 두 개의 스테이지의 각각은 다음 연산: 제1 AddRoundKey, S-박스, P-박스 및 제2 AddRoundKey를 통해 데이터를 전달한다.
- [0011] 더 바람직하게는, 상기 AddRoundKey 레이어는 상기 128 비트 사용자 입력 키를 위해 상기 8개의 라운드의 각 라운드마다 고유한 128 비트 라운드 키를 생성하고, 상기 라운드 키를 32 비트로 이루어지는 네 개의 키로 나누어 상기 두 개의 스테이지의 각각이 각각 두 개의 키를 사용하도록 구성되고, 상기 S-박스 레이어는 상기 사용자 입력 데이터의 입력 비트들의 치환을 수행함으로써 입력의 변환된 값을 나타내는 출력 비트들의 값을 갖는 출력 비트에 맵핑하도록 구성되며, 상기 P-박스 레이어는 상기 S-박스 레이어의 출력 비트들을 입력으로서 사용하는 32 대 1 다중화기들로 이루어지고, 16 비트 가변 키가 상기 다중화기들에 대한 선택 신호들로서의 역할을 하며, 두 개의 다중화기가 상기 16 비트 가변 키로부터의 하나의 선택 신호에 의해 제어되도록 구성된다.
- [0012] 훨씬 더 바람직하게는, 상기 AddRoundKey 레이어는 먼저 상기 사용자 입력 키를 라운드 1의 라운드 키로 생성하고, 그 다음 라운드 i (여기서, $i=1, 2, \dots, 8$)의 라운드 키를 직전 라운드 $i-1$ 의 직전 라운드 키를 25 비트만큼 순환 시프트시켜 각 라운드에 대해 고유한 상기 라운드 키들을 생성한다.
- [0013] 훨씬 더 바람직하게는, 상기 P-박스 레이어는 상기 각 스테이지에 대해 상기 라운드 키의 절반을 사용하여 배타적-or 연산함으로써 상기 16 비트 가변 키를 생성한다.

발명의 효과

- [0014] 상술한 바와 같이, 본 발명에 의한 퍼베이션 컴퓨팅을 위한 효과적인 초경량 블록 암호 시스템은 다음과 같은 효과를 제공한다.
- [0015] 새로운 경량 블록 암호의 설계 및 구현에 초점을 두고 치환-순열(S-P) 네트워크와 파이스텔 구조의 장단점을 연구하여, 두 가지 네트워크의 이용시 가장 적합한 방향을 제시함으로써, 작은 하드웨어 면적을 가지면서도 높은 처리량 암호화 알고리즘을 요구하는 퍼베이션 컴퓨팅에 매우 적합한 초경량 블록 암호를 제공한다.
- [0016] 이와 같이, 본 발명은 퍼베이션 컴퓨팅의 보안 모듈 구현 비용을 줄일 수 있다. 따라서, 본 발명은 저면적 및 높은 처리량에서 기인하는 제약을 갖는 장치에서 민감한 데이터를 보호할 때 매우 효율적이다.

도면의 간단한 설명

- [0017] 도 1은 본 발명의 바람직한 실시예에 따른 초경량 블록 암호 시스템의 암호화 루틴의 상위 레벨 알고리즘을 나타내는 모식도이다.
- 도 2는 본 발명의 바람직한 실시예에 따른 초경량 블록 암호 시스템의 복호화 루틴의 상위 레벨 알고리즘을 나타내는 모식도이다.
- 도 3은 본 발명의 바람직한 실시예에 따른 초경량 블록 암호 시스템의 암호화 루틴의 키 스케줄 알고리즘을 나타내는 모식도이다.
- 도 4는 본 발명의 바람직한 실시예에 따른 초경량 블록 암호 시스템의 복호화 루틴의 키 스케줄 알고리즘을 나타내는 모식도이다.
- 도 5는 본 발명의 바람직한 실시예에 따른 AddRoundKey 연산 방법을 나타내는 모식도이다.

도 6은 본 발명의 바람직한 실시예에 따른 P-박스의 출력들을 생성하기 위한 알고리즘을 나타내는 도면이다.

도 7은 본 발명의 예시적인 실험예에 따른 초경량 블록 암호의 암호화/복호화 코어의 시뮬레이션 결과들을 도시하는 도면이다.

도 8은 본 발명의 예시적인 실험예에 따른 초경량 블록 암호 시스템에서의 원본 이미지, 암호화된 이미지 및 복호화된 이미지를 나타내는 도면이다.

발명을 실시하기 위한 구체적인 내용

- [0018] 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나 본 발명은 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 실시예들은 본 발명의 개시가 완전하도록 하고, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다.
- [0019] 이하 본 발명의 퍼베이션 컴퓨팅을 위한 효과적인 초경량 블록 암호 시스템에 대하여 첨부된 도면을 참조하여 상세히 설명하기로 한다.
- [0020] 1. 암호화/복호화 알고리즘 설명
- [0021] 본 발명의 바람직한 실시예에 따른 초경량 블록 암호 시스템은 경량화를 위해 오직 메모리의 64 비트를 요구하는 S-박스과 키-의존 원 스테이지 오메가 순열 네트워크 구조를 사용하는 P-박스과 함께, 암호화와 복호화를 위한 하나의 코어 실행을 가능하게 하는 파이스텔 구조를 사용한다.
- [0022] 본 발명의 바람직한 실시예에 따른 초경량 블록 암호 시스템은 64 비트 사용자 입력 데이터 및 128 비트 사용자 입력 키를 취하고, 각 라운드가 오로지 두 개의 수학적 연산자(Shift, XOR)를 사용하여 생성되는 새로운 라운드 키를 사용하는 8개의 라운드로 이루어진다. 각 라운드는 두 개의 스테이지로 이루어진다. 제1 스테이지는 다음 4개의 연산을 통해 데이터를 전달한다: 제1 AddRoundKey, S-박스, P-박스 및 제2 AddRoundKey. 제2 스테이지는 단지 사용되는 키들이 달라진다는 점을 제외하고는, 제1 스테이지와 동일한 세트의 연산으로 이루어진다. 그 결과, 본 발명의 바람직한 실시예에 따른 초경량 블록 암호는 8개의 라운드에서 데이터를 암호화하기 위해 128 비트 키를 사용하는 64 비트 블록 암호이다.
- [0023] 도 1은 본 발명의 초경량 블록 암호 시스템의 암호화 루틴의 상위 레벨 알고리즘 설명을 도시하고, 도 2는 본 발명의 바람직한 실시예에 따른 초경량 블록 암호 시스템의 복호화 루틴의 상위 레벨 알고리즘 설명을 도시한다.
- [0024] 2. AddRoundKey 레이어
- [0025] 키 스케줄 알고리즘
- [0026] 본 발명의 초경량 블록 암호 시스템은 무차별 대입 공격(brute force attack)을 무력화시키기에 충분한 128 비트 키를 사용한다.
- [0027] 퍼베이션 컴퓨팅을 위한 키 스케줄 알고리즘을 구현하는 데 있어서, 성능이 보안보다 중시된다. 본 발명의 초경량 블록 암호 시스템의 설계에서, 키 스케줄 알고리즘을 설계하기 전 고려되는 몇몇 사항은 다음을 포함한다: i) 키 스케줄 알고리즘은 극히 간단해야 한다, ii) 키 스케줄 알고리즘은 빨라야 한다, 그리고 iii) 키 스케줄 알고리즘은 최소한의 하드웨어 자원들을 사용해야 한다.
- [0028] 키 스케줄을 위해, 본 발명의 AddRoundKey 레이어(100)는 먼저 128 비트의 사용자 제공 입력 키를 레지스터에 저장한다.
- [0029] 그리고 암호화 루틴을 위한 키 스케줄 알고리즘은 도 3에 도시된 바와 같은 한편, 복호화 루틴을 위한 키 스케줄 알고리즘은 도 4에 도시된다. 암호화 루틴에 대해, 도 2를 참조하여 본 발명의 키 스케줄 알고리즘은 128 비트의 사용자 입력 키를 취해 8개의 라운드(ROUND₁...ROUND₈)의 각 라운드마다 새로운 라운드 키(KEY₁...KEY₈)를 생성한다. 구체적으로, 먼저 사용자 입력 키를 라운드 1의 라운드 키(KEY₁)로 설정하고, 그 다음 라운드 i의 라운드 키(KEY_i)를 직전 라운드 i-1의 직전 라운드 키(KEY_{i-1})의 내용을 25 비트만큼 왼쪽으로 회전시키며, 이를 각 라운드마다 반복한다. 복호화 루틴에 대해서는, 도 3을 참조하여 단지 왼쪽으로 회전하는 연산 대신 오른쪽

으로 회전하는 연산을 수행한다는 점을 제외하고는, 암호화 루틴에 대해서와 동일하다.

[0030] 본 발명의 키 스케줄 알고리즘이 단지 순환 시프트 연산들만을 수반하기 때문에, 그것은 구현을 위해 극히 소수의 하드웨어 자원만을 필요로 한다. 또한, 암호화 및 복호화의 각 라운드마다 완전히 고유한 키가 생성된다. 이는 키 스케줄 알고리즘을 해독하려는 관련 키 공격들의 사용을 무력화시킬 수 있다.

[0031] AddRoundKey 연산

[0032] 그 다음, 본 발명의 AddRoundKey 레이어(100)는 키 스케줄 알고리즘에 의해 생성된 각 라운드에 완전히 고유한 128 비트 키(KEY)를 네 개의 키(K0, K1, K2 및 K3)로 나눈다. 네 개의 키의 각각은 32 비트로 이루어진다. 128 비트 키(KEY)는 다음과 같은 네 개의 키 위치에 할당된다: $K0=K[31:0]$, $K1=K[63:32]$, $K2=K[95:64]$, $K3=K[127:96]$. 암호화 루틴에 대해, 각 라운드에서의 스테이지 1은 K0 및 K1을 사용하는 한편 각 라운드에서의 스테이지 2는 K2 및 K3을 사용하고, 복호화 루틴에 대해, 각 라운드에서의 스테이지 1은 K2 및 K3을 사용하는 한편 각 라운드에서의 스테이지 2는 K0 및 K1을 사용한다.

[0033] 그리고 간단한 배타적 논리합(XOR)인 AddRoundKey 연산이 알고리즘의 각 라운드에서 4번 적용된다. 32 비트 키 ($K=K_{31} \dots K_0$) 및 현재 상태($S=S_{31} \dots S_0$)가 주어질 때, AddRoundKey 연산 방법이 도 5에 도시된다.

[0034] 3. S-박스 레이어

[0035] 대칭 키 알고리즘들에서, 치환-박스(Substitution-box, S-박스)(200)는 AddRoundKey 레이어(100)에 의해 생성된 키 및 암호문 간 관계를 마스킹(masking)하기 위해, 비트들의 치환을 수행하는 기본적인 구성요소이다. 일반적으로, S-박스(200)는 여러 입력 비트를 취하고, 그것을 입력의 변환된 값을 나타내는 출력 비트들의 값을 갖는 여러 출력 비트에 맵핑한다. 특히, 본 발명의 바람직한 실시예에 따른 초경량 블록 암호 시스템에서는 백도어 아이디어가 암호화 알고리즘에 사용되는 것을 방지하기 위해, 당해 기술분야에 공지된 PRESENT 알고리즘의 S-박스(200)를 채용한다. PRESENT S-박스(200)는 선형 및 차분 해독법 양자에 강하다.

[0036] 표 2는 본 발명의 바람직한 실시예에 따른 초경량 블록 암호 시스템에 의해 사용되는 PRESENT S-박스(200)를 제시한다. S-박스(200)는 4 비트 S-박스(S)에 대해 4 비트이다: $F_2^4 \rightarrow F_2^4$.

[0037] 본 발명의 S-박스 레이어(200)에 대해, 현재 상태($S_{31} \dots S_0$)는 4 비트 워드($W_7 \dots W_0$)인 것으로 고려되며, 여기서 $W_i = S_{4i+3} || S_{4i+2} || S_{4i+1} || S_{4i}$, 단 $0 \leq i \leq 7$ 이다. 니블(nibble) $S[W_i]$ 는 업데이트된 상태를 제공한다. 암호화 알고리즘 및 해독화 알고리즘은 동일한 S-박스(200)를 사용한다.

표 2

[0038]

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S[x]	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

[0039] 4. P-박스 레이어

[0040] 암호 기법에서, 순열 박스(Permutation-box, P-박스)는 S-박스 입력들에 걸쳐 비트들을 순열로 배치하기 위해 사용된다. P-박스가 면밀하게 구현되는 경우, S-박스들의 출력들이 가능한 많은 P-박스 입력으로 분배된다. S-박스 레이어가 순열-치환(S-P) 네트워크 클록 암호의 가장 중요한 부분이지만, P-박스는 암호의 엄격한 애벌란시 기준(Strict Avalanche Criterion, SAC)을 충족시키는 데 필수적이다. 엄격한 애벌란시 기준은 단일 입력 비트가 반전되며, 각 출력 비트가 50%의 확률로 바뀌면 충족된다.

[0041] 종래 기술의 많은 블록 암호는 고정 P-박스를 사용한다. 그러나 차분 및 선형 해독법의 출현으로, 고정 P-박스는 더 이상 안전하지 않다. 이에 전혀 새로운 유형의 P-박스(300)가 본 출원에서 제안된다. 본 출원에서 제안되는 P-박스(300)는 키 의존 원 스테이지 오메가 순열 네트워크이다.

[0042] 도 6에 도시된 바와 같이, 본 발명의 초경량 블록 암호 시스템의 P-박스 레이어(300)는 S-박스 레이어(200)의 출력들을 입력으로서 사용하는 32대 1 다중화기로 이루어진다. 16 비트 가변 키(KEY_BITS)가 다중화기들에 대한 선택 신호들로서의 역할을 하고, 두 개의 다중화기가 (KEY_BITS로부터의) 하나의 선택 신호에 의해 제어된다.

[0043] 암호화 루틴에 대해, 각 라운드에서의 스테이지 1은 다음과 같이 KEY_BITS를 계산하기 위해 128 비트 라운드 키

(KEY)의 하반부(K0 및 K1)(KEY[63:0])가 사용한다: $KEY_BITS[15:0] = KEY[63:48] \wedge KEY[47:32] \wedge KEY[31:16] \wedge KEY[15:0]$, 여기서 연산자($\wedge$)는 배타적-or(exclusive-or) 연산자이다. 한편 각 라운드에서의 스테이지 2는 128 비트 라운드 키(KEY)의 상단부(K2 및 K3)를 사용하고, 복호화 루틴에 대해, 각 라운드에서의 스테이지 1은 K2 및 K3을 사용하는 한편 각 라운드에서의 스테이지 2는 K0 및 K1을 사용한다.

[0044] P-박스의 출력들을 생성하기 위한 알고리즘이 도 6에 도시된다. 알고리즘에서, in_data[31:0]은 S-박스의 출력들을 나타내는 한편, pbox[31:0]은 P-박스의 출력을 나타낸다. 여기서 다시, 암호화 알고리즘 및 해독화 알고리즘은 동일한 P-박스를 사용한다.

[0046] 실험예

[0047] 본 발명에서 개시된 초경량 블록 암호 시스템의 성능을 평가하기 위해, virtex 6 FPGA를 구비한 iNEXT-V6 보드 상에 Xilinx ISE 143을 사용하여 설계를 통합했다. 시뮬레이션을 위해 Mentor Graphics Modelsim SE 64 10.1c를 사용했다. 도 7은 본 발명에서 개시된 초경량 블록 암호의 암호화/복호화 코어의 시뮬레이션 결과들을 도시한다. 도 7로부터 각 암호화 및 복호화 루틴들마다 단지 8개의 클록 사이클을 취함을 알 수 있다. 다른 알고리즘들과 비교한 본 발명에서 개시된 초경량 블록 암호 알고리즘 하드웨어 결과들을 표 3에 나타냈다.

표 3

설계	최대 지연 (ns)	블록당 클록 사이클	블록 사이즈 (비트)	키 사이즈 (비트)	영역 (슬라이스)	스루풋 (Mbps)	영역당 Mbps (Mbps/슬라이스)
PRESENT	394	32	64	128	202	508	2.5
AES	20.00	46	128	128	222	139	0.62
CLEPIA	5.4	36	128	128	270	658	2.40
Camellia	7.95	875	128	128	318	18.41	0.06
Tiny XTEA	15.97	112	64	128	254	35.78	0.14
본 발명	2.97	8	64	128	196	2693	13.76

[0049] 1. 이미지 암호화/복호화 어플리케이션

[0050] 본 실험예에서, 본 발명에서 개시된 초경량 블록 암호 시스템의 이미지 암호화 및 복호화를 수행하기 위한 실시간 처리 성능을 평가했다. 실험은 iNEXT-V6 테스트 보드 상에서 수행했다. 테스트 이미지는 480x272 JPEG 포맷의 인물 이미지이다. 본 실험예에서, 먼저 이미지를 COE 파일로 변환하고 온-칩 블록 ROM에 저장했다. ROM으로부터의 데이터를 암호화할 암호화 모듈로 전송했다. 암호화된 데이터는 RAM에 저장하고 데이터를 복호화할 복호화 모듈로 전송했다. 복호화된 데이터를 또한 RAM에 저장했다. 원본 이미지, 암호화된 이미지 및 복호화된 이미지가 iNEXT-V6 테스트 보드의 TFT LCD 상에 차례로 디스플레이된다. TFT LCD 상에 디스플레이되는 이미지가 도 8에 도시된다.

[0051] 이미지의 암호화 및 복호화 양자에 걸린 시간을 조사하기 위해, 시뮬레이션의 클록 기간을 10ns로 설정했고 전체 암호화 및 복호화에 걸린 시간을 측정했다. 다른 알고리즘들과 비교한 본 명세서에서 개시된 암호화/복호화 어플리케이션 결과들을 표 4에 나타냈다.

표 4

알고리즘	이미지 사이즈 (픽셀)	클록 기간 (ns)	사이클/블록	암호화/복호화에 소 요된 시간(s)
AES	480X272	10	46	0.120
PRESENT	480X272	10	32	0.080
TEA	480X272	10	64	0.160
본 발명	480X272	10	8	0.021

[0053] 2. 애벌란시 효과 조사

[0054] 다음에서, 본 발명의 초경량 블록 암호 시스템에 대한 10개의 테스트 벡터를 제공한다. 여기서, 암호 키 "ABCDEFG20758191 AD185DABF04954C78A"는 일정하게 유지되나, 평문은 1 비트씩 바뀐다. 이는 새로운 암호의 애벌란시 특성을 테스트하기 위한 것이다. 해밍 거리(평문이 하나씩 상이한 두 개의 암호문에서의 비트 변화)를 두 개의 암호문의 배타적-or 연산하여 계산했다. 모든 데이터는 16진법으로 표현된다.

표 5

평문	암호문	해밍 거리
0000 0000 0000 0000	DOEBBF002FC221E	28
0000 0000 0000 0001	A8013D5725FC8496	
0000 0000 0000 0002	1B9A72BACD398D34	
0000 0000 0000 0003	D25667B09B4DB802	29
0000 0000 0000 0004	936F3EDA60197859	
0000 0000 0000 0005	8959DC899621A7CF	35
0000 0000 0000 0006	EB5B8A40466BAEC6	
0000 0000 0000 0007	A88459CA673E9FA2	30
0000 0000 0000 0008	8906477C8E40B4C7	
0000 0000 0000 0009	45AF2659DDC09CF5	24

[0056] 본 발명의 초경량 블록 암호 시스템 구현 결과, 196 슬라이스를 필요로 하는 한편 337 MHz의 최대 주파수를 제공한다. 암호가 극히 소수의 하드웨어(RFID 태그와 같은 제약을 갖는 디바이스)를 사용하도록 설계되었지만, 그것은 동일하게 고속 및 높은 스루풋 어플리케이션에 바람직하다. 본 발명의 초경량 블록 암호 시스템의 설계는 매우 간단하지만 암호 기법에서 사용되는 많은 기술을 통합한다.

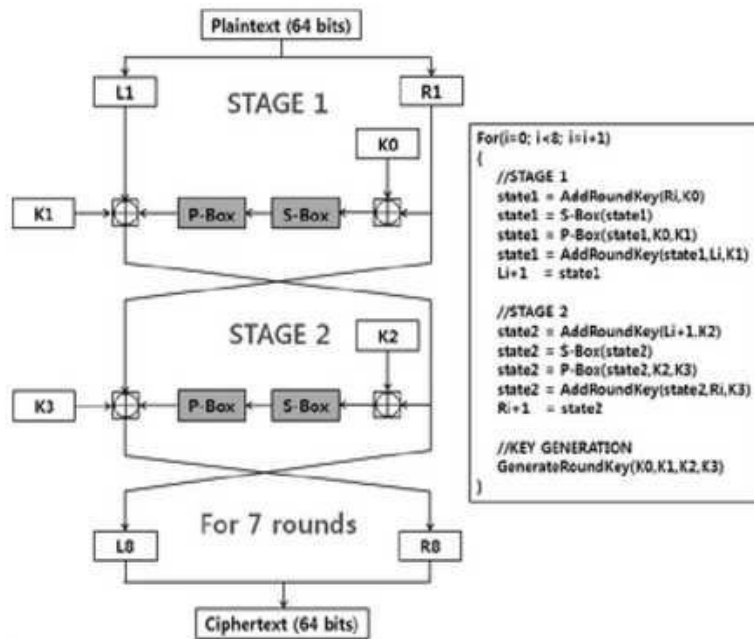
[0057] 이상에서 몇 가지 실시예를 들어 본 발명을 더욱 상세하게 설명하였으나, 본 발명은 반드시 이러한 실시예로 국한되는 것은 아니고 본 발명의 기술사상을 벗어나지 않는 범위 내에서 다양하게 변형 실시될 수 있다.

부호의 설명

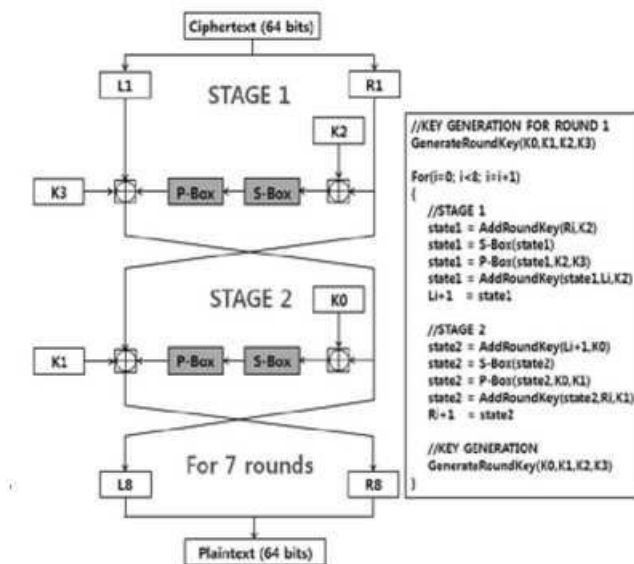
[0058] 100 : AddRoundKey 레이어
200 : S-박스 레이어
300 : P-박스 레이어

도면

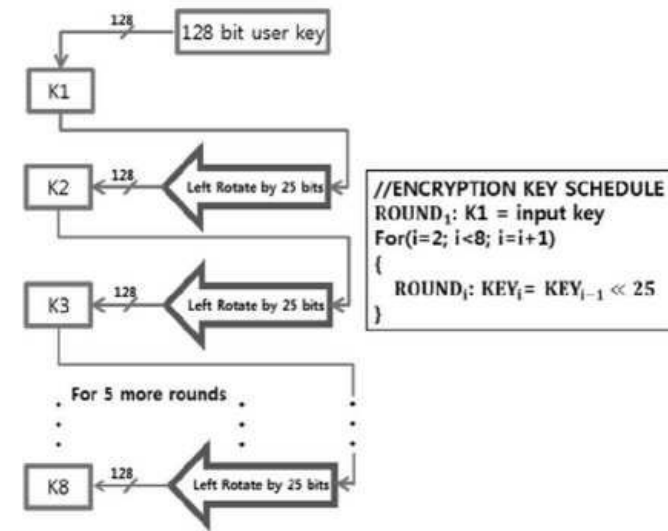
도면1



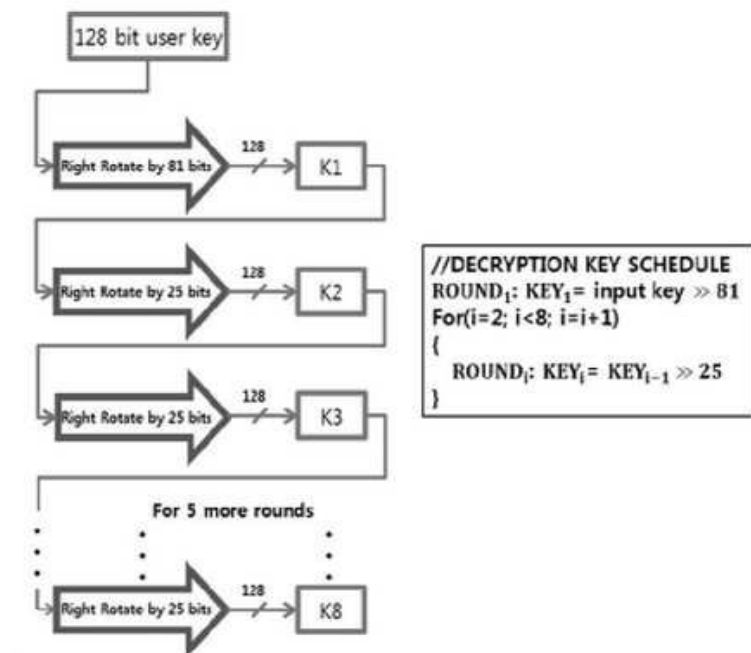
도면2



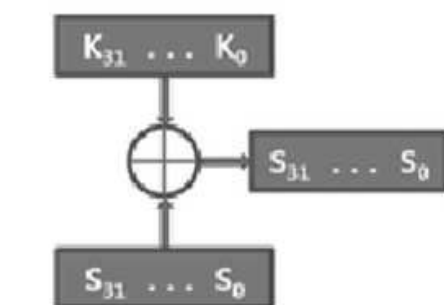
도면3



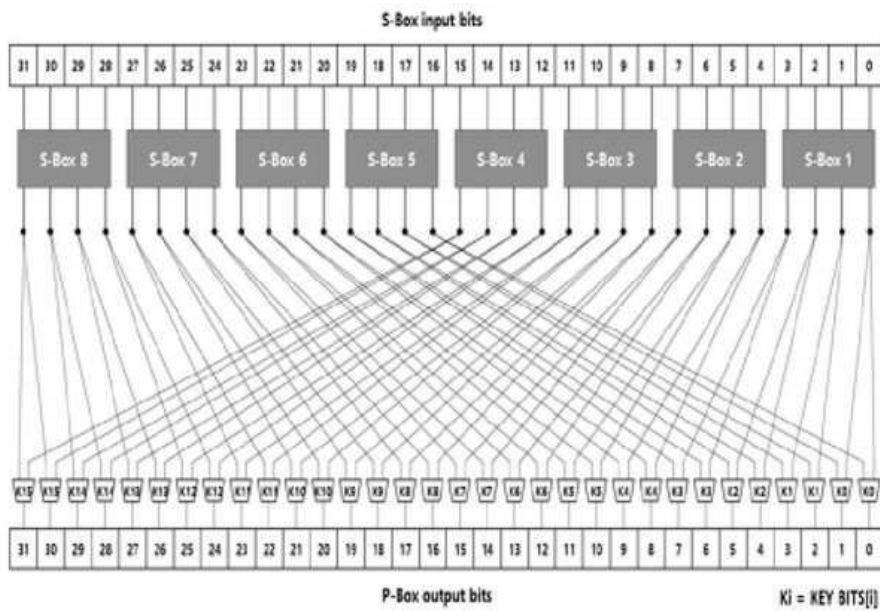
도면4



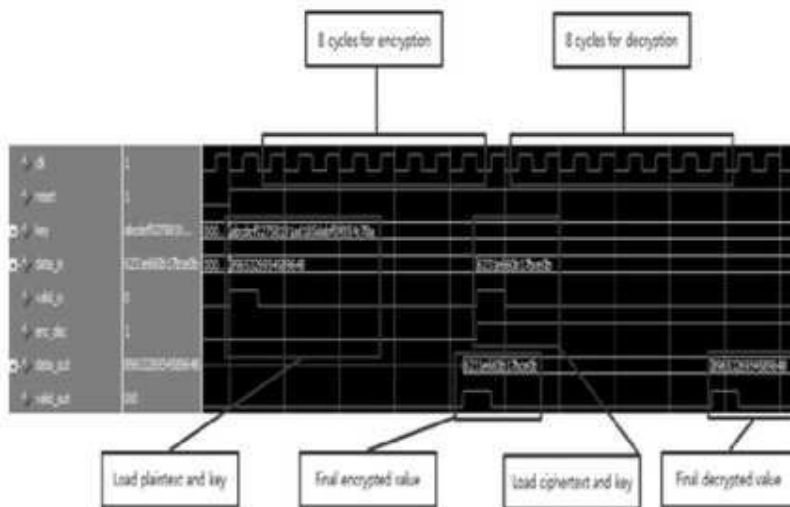
도면5



도면6



도면7



도면8

