(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2015-0105405
(43) 공개일자 2015년09월16일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *H04L 9/06* (2006.01)
(52) CPC특허분류
H04L 9/0816 (2013.01)
H04L 9/0631 (2013.01)
(21) 출원번호 10-2015-7021223
(22) 출원일자(국제) 2013년12월27일
심사청구일자 없음
(85) 번역문제출일자 2015년08월05일
(86) 국제출원번호 PCT/US2013/077939
(87) 국제공개번호 WO 2014/109918
국제공개일자 2014년07월17일
(30) 우선권주장
61/751,541 2013년01월11일 미국(US)
13/935,962 2013년07월05일 미국(US)

(71) 출원인
퀄컴 인코포레이티드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
로즈, 그레고리 고든
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(74) 대리인
특허법인 남앤드남

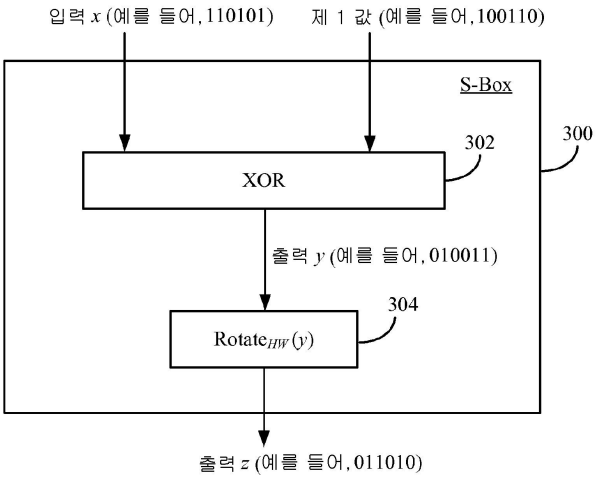
전체 청구항 수 : 총 28 항

(54) 발명의 명칭 **컴퓨팅 가능하고, 대형이며, 가변적이며 안전한 치환 박스를 위한 방법 및 장치**

(57) 요 약

하나의 특징은 S-박스(substitution box)와 연관되는 암호 값들을 생성하기 위한 방법에 관한 것이다. 방법들은 우선, 입력 값 및 제 1 값을 획득하는 단계를 포함한다. 일 방법은 중간 값을 생성하기 위해 입력 값 및 제 1 값에 대해 배타적 OR(XOR) 동작을 수행하고 중간 값의 해밍 웨이트(Hamming Weight)와 동일한 비트들의 수 만큼 중간 값에 대해 비트와이즈 회전을 수행함으로써 S-박스 출력 값을 생성하는 단계를 포함한다. 일 양상에서, 비트와이즈 회전의 출력은 추가로 제 2 값과 XOR된다. 다른 방법은 중간 값을 생성하기 위해 상기 입력 값의 해밍 웨이트와 동일한 비트들의 수 만큼 입력 값에 대해 비트와이즈 회전을 수행하고 중간 값 및 제 1 값에 대해 XOR 동작을 수행함으로써 S-박스 출력 값을 생성하는 단계를 포함한다.

대 표 도 - 도3



명 세 서

청구범위

청구항 1

S-박스(substitution box)와 연관되는 암호 값들을 생성하기 위한 방법으로서,

입력 값 및 제 1 값을 획득하는 단계; 및

(A) 제 1 중간 값을 생성하기 위해 상기 입력 값 및 상기 제 1 값에 대해 비트와이즈 배타적 OR(XOR) 동작을 수행하는 것, 및

상기 S-박스 출력 값을 생성하기 위해 상기 제 1 중간 값의 해밍 웨이트(Hamming Weight)와 동일한 비트들의 수 만큼 상기 제 1 중간 값에 대해 비트와이즈 회전 동작을 수행하는 것;

(B) 상기 제 1 중간 값을 생성하기 위해 상기 입력 값의 해밍 웨이트와 동일한 비트들의 수 만큼 상기 입력 값에 대해 비트와이즈 회전 동작을 수행하는 것, 및

상기 S-박스 출력 값을 생성하기 위해 상기 제 1 중간 값 및 상기 제 1 값에 대해 비트와이즈 XOR 동작을 수행하는 것, 또는

(C) 상기 제 1 중간 값을 생성하기 위해 상기 입력 값 및 상기 제 1 값에 대해 비트와이즈 XOR 동작을 수행하는 것,

제 2 중간 값을 생성하기 위해 상기 제 1 중간 값의 해밍 웨이트와 동일한 비트들의 수 만큼 상기 제 1 중간 값에 대해 비트와이즈 회전 동작을 수행하는 것,

제 2 값을 획득하는 것, 및

상기 S-박스 출력 값을 생성하기 위해 상기 제 2 중간 값 및 상기 제 2 값에 대해 비트와이즈 XOR 동작을 수행하는 것,

중 하나에 의해, S-박스 출력 값을 생성하는 단계를 포함하는,

S-박스와 연관되는 암호 값들을 생성하기 위한 방법.

청구항 2

제 1 항에 있어서,

제공된 상기 제 1 값 및/또는 제 2 값 중 적어도 하나는 50%와 같거나 그 초과의 확률로 상기 입력 값과 상이한 해밍 웨이트를 갖는 S-박스 출력 값을 생성하도록 구성되는,

S-박스와 연관되는 암호 값들을 생성하기 위한 방법.

청구항 3

제 1 항에 있어서,

상기 제 1 값 및/또는 상기 제 2 값 중 적어도 하나는 비-제로(non-zero) 해밍 웨이트를 갖는 상수인,

S-박스와 연관되는 암호 값들을 생성하기 위한 방법.

청구항 4

제 1 항에 있어서,

제공된 상기 제 1 값 및/또는 제 2 값 중 적어도 하나는 가변적이며 $100*(1-2^{-n})$ 퍼센트와 같거나 그 초과의, 비-제로 해밍 웨이트를 가질 확률을 가지며, 여기서 n은 상기 제 1 값 및/또는 제 2 값의 비트들의 수인,

S-박스와 연관되는 암호 값들을 생성하기 위한 방법.

청구항 5

제 1 항에 있어서,

상기 제 1 값 및/또는 상기 제 2 값 중 적어도 하나는 암호 함수 및/또는 암호 키 중 적어도 하나로부터 유도되는,

S-박스와 연관되는 암호 값들을 생성하기 위한 방법.

청구항 6

제 1 항에 있어서,

상기 제 1 값 및/또는 상기 제 2 값 중 적어도 하나는 암호 모듈의 컴포넌트 스테이지로부터 유도되는,

S-박스와 연관되는 암호 값들을 생성하기 위한 방법.

청구항 7

제 6 항에 있어서,

상기 암호 모듈은 스트림 암호인,

S-박스와 연관되는 암호 값들을 생성하기 위한 방법.

청구항 8

제 1 항에 있어서,

상기 방법은 메모리 회로에서 실행되는,

S-박스와 연관되는 암호 값들을 생성하기 위한 방법.

청구항 9

제 1 항에 있어서,

상기 입력 값 및 상기 S-박스 출력 값은 동일한 비트들의 수를 갖는,

S-박스와 연관되는 암호 값들을 생성하기 위한 방법.

청구항 10

제 1 항에 있어서,

메인 입력 값을 획득하는 단계;

복수의 NLTF(non-linear transformation function) 입력 값들을 획득하도록 상기 메인 입력 값의 비트들을 배분하는 단계 - 각각의 NLTF 입력 값은 상기 메인 입력 값의 비트들의 수 미만인 비트들의 수를 가짐 - ;

상기 NLTF에 제공되는 NLTF 입력 값에 각각 대응하는 복수의 NLTF 출력 값들을 생성하도록 비-선형 동작을 실행하는 NLTF에 상기 NLTF 입력 값들 각각을 제공하는 단계; 및

상기 입력 값을 획득하도록 상기 복수의 NLTF 출력 값들을 연계(concatenating)하는 단계

를 더 포함하는,

S-박스와 연관되는 암호 값들을 생성하기 위한 방법.

청구항 11

제 10 항에 있어서,

상기 메인 입력 값은 상기 복수의 NLTF 입력 값들 각각이 동일한 비트들의 수를 갖도록 배분되는,

S-박스와 연관되는 암호 값들을 생성하기 위한 방법.

청구항 12

전자 디바이스로서,

프로세싱 회로를 포함하고,

상기 프로세싱 회로는,

입력 값 및 제 1 값을 획득하도록; 그리고

(A) 제 1 중간 값을 생성하기 위해 상기 입력 값 및 상기 제 1 값에 대해 비트와이즈 배타적 OR(XOR) 동작을 수행하는 것, 및

상기 S-박스 출력 값을 생성하기 위해 상기 제 1 중간 값의 해밍 웨이트(Hamming Weight)와 동일한 비트들의 수 만큼 상기 제 1 중간 값에 대해 비트와이즈 회전 동작을 수행하는 것;

(B) 상기 제 1 중간 값을 생성하기 위해 상기 입력 값의 해밍 웨이트와 동일한 비트들의 수 만큼 상기 입력 값에 대해 비트와이즈 회전 동작을 수행하는 것, 및

상기 S-박스 출력 값을 생성하기 위해 상기 제 1 중간 값 및 상기 제 1 값에 대해 비트와이즈 XOR 동작을 수행하는 것, 또는

(C) 상기 제 1 중간 값을 생성하기 위해 상기 입력 값 및 상기 제 1 값에 대해 비트와이즈 XOR 동작을 수행하는 것,

제 2 중간 값을 생성하기 위해 상기 제 1 중간 값의 해밍 웨이트와 동일한 비트들의 수 만큼 상기 제 1 중간 값에 대해 비트와이즈 회전 동작을 수행하는 것,

제 2 값을 획득하는 것, 및

상기 S-박스 출력 값을 생성하기 위해 상기 제 2 중간 값 및 상기 제 2 값에 대해 비트와이즈 XOR 동작을 수행하는 것,

중 하나에 의해, S-박스 출력 값을 생성하도록 구성되는,

전자 디바이스.

청구항 13

제 12 항에 있어서,

제공된 상기 제 1 값 및/또는 제 2 값 중 적어도 하나는 50%와 같거나 그 초과의 확률로 상기 입력 값과 상이한 해밍 웨이트를 갖는 S-박스 출력 값을 생성하도록 구성되는,

전자 디바이스.

청구항 14

제 12 항에 있어서,

상기 제 1 값 및/또는 상기 제 2 값 중 적어도 하나는 비-제로(non-zero) 해밍 웨이트를 갖는 상수인,

전자 디바이스.

청구항 15

제 12 항에 있어서,

제공된 상기 제 1 값 및/또는 제 2 값 중 적어도 하나는 가변적이고 $100*(1-2^{-n})$ 퍼센트와 같거나 그 초과의, 비-제로 해밍 웨이트를 가질 확률을 가지며, 여기서 n은 상기 제 1 값 및/또는 제 2 값의 비트들의 수인,

전자 디바이스.

청구항 16

제 12 항에 있어서,

상기 제 1 값 및/또는 상기 제 2 값 중 적어도 하나는 암호 함수 및/또는 암호 키 중 적어도 하나로부터 유도되는,

전자 디바이스.

청구항 17

제 12 항에 있어서,

상기 제 1 값 및/또는 상기 제 2 값 중 적어도 하나는 암호 모듈의 컴포넌트 스테이지로부터 유도되는,

전자 디바이스.

청구항 18

제 12 항에 있어서,

상기 프로세싱 회로는 추가로,

메인 입력 값을 획득하도록;

복수의 NLTF(non-linear transformation function) 입력 값들을 획득하도록 상기 메인 입력 값의 비트들을 배분하도록 - 각각의 NLTF 입력 값은 상기 메인 입력 값의 비트들의 수 미만인 비트들의 수를 가짐 - ;

상기 NLTF에 제공되는 NLTF 입력 값에 각각 대응하는 복수의 NLTF 출력 값들을 생성하도록 비-선형 동작을 실행하는 NLTF에 상기 NLTF 입력 값들 각각을 제공하도록; 그리고

상기 입력 값을 획득하도록 상기 복수의 NLTF 출력 값들을 연계하도록

구성되는,

전자 디바이스.

청구항 19

전자 디바이스로서,

입력 값 및 제 1 값을 획득하기 위한 수단; 및

(A) 제 1 중간 값을 생성하기 위해 상기 입력 값 및 상기 제 1 값에 대해 비트와이즈 배타적 OR(XOR) 동작을 수행하기 위한 수단, 및

상기 S-박스 출력 값을 생성하기 위해 상기 제 1 중간 값의 해밍 웨이트(Hamming Weight)와 동일한 비트들의 수 만큼 상기 제 1 중간 값에 대해 비트와이즈 회전 동작을 수행하기 위한 수단;

(B) 상기 제 1 중간 값을 생성하기 위해 상기 입력 값의 해밍 웨이트와 동일한 비트들의 수 만큼 상기 입력 값에 대해 비트와이즈 회전 동작을 수행하기 위한 수단, 및

상기 S-박스 출력 값을 생성하기 위해 상기 제 1 중간 값 및 상기 제 1 값에 대해 비트와이즈 XOR 동작을 수행하기 위한 수단, 또는

(C) 상기 제 1 중간 값을 생성하기 위해 상기 입력 값 및 상기 제 1 값에 대해 비트와이즈 XOR 동작을 수행하기 위한 수단,

제 2 중간 값을 생성하기 위해 상기 제 1 중간 값의 해밍 웨이트와 동일한 비트들의 수 만큼 상기 제 1 중간 값에 대해 비트와이즈 회전 동작을 수행하기 위한 수단,

제 2 값을 획득하기 위한 수단, 및

상기 S-박스 출력 값을 생성하기 위해 상기 제 2 중간 값 및 상기 제 2 값에 대해 비트와이즈 XOR 동작을 수행하기 위한 수단,

중 하나에 의해, S-박스 출력 값을 생성하기 위한 수단을 포함하고,

전자 디바이스.

청구항 20

제 19 항에 있어서,

제공된 상기 제 1 값 및/또는 제 2 값 중 적어도 하나는 50%와 같거나 그 초과의 확률로 상기 입력 값과 상이한 해밍 웨이트를 갖는 S-박스 출력 값을 생성하도록 구성되는,

전자 디바이스.

청구항 21

제 19 항에 있어서,

상기 제 1 값 및/또는 상기 제 2 값 중 적어도 하나는 비-제로(non-zero) 해밍 웨이트를 갖는 상수인,

전자 디바이스.

청구항 22

제 19 항에 있어서,

상기 제 1 값 및/또는 상기 제 2 값 중 적어도 하나는 암호 함수 및/또는 암호 키 중 적어도 하나로부터 유도되는,

전자 디바이스.

청구항 23

제 19 항에 있어서,

상기 제 1 값 및/또는 상기 제 2 값 중 적어도 하나는 암호 모듈의 컴포넌트 스테이지로부터 유도되는,

전자 디바이스.

청구항 24

제 19 항에 있어서,

메인 입력 값을 획득하기 위한 수단;

복수의 NLTF(non-linear transformation function) 입력 값들을 획득하기 위해 상기 메인 입력 값의 비트들을 배분하기 위한 수단 - 각각의 NLTF 입력 값은 상기 메인 입력 값의 비트들의 수 미만인 비트들의 수를 가짐 -;

상기 NLTF에 제공되는 NLTF 입력 값에 각각 대응하는 복수의 NLTF 출력 값들을 생성하기 위해 비-선형 동작을 실행하는 NLTF에 상기 NLTF 입력 값들 각각을 제공하기 위한 수단; 및

상기 입력 값을 획득하기 위해 상기 복수의 NLTF 출력 값들을 연계하기 위한 수단

을 더 포함하는,

전자 디바이스.

청구항 25

S-박스(substitution box)와 연관된 암호 값을 생성하기 위한 명령들이 저장되어 있는 컴퓨터-판독 가능한 저장 매체로서, 상기 명령은 적어도 하나의 프로세서에 의해 실행될 때, 상기 프로세서로 하여금,

입력 값 및 제 1 값을 획득하게 하고, 그리고

(A) 제 1 중간 값을 생성하기 위해 상기 입력 값 및 상기 제 1 값에 대해 비트와이즈 배타적 OR(XOR) 동작을 수행하는 것, 및

상기 S-박스 출력 값을 생성하기 위해 상기 제 1 중간 값의 해밍 웨이트(Hamming Weight)와 동일한 비트들의 수

만큼 상기 제 1 중간 값에 대해 비트와이즈 회전 동작을 수행하는 것;

(B) 상기 제 1 중간 값을 생성하기 위해 상기 입력 값의 해밍 웨이트와 동일한 비트들의 수 만큼 상기 입력 값에 대해 비트와이즈 회전 동작을 수행하는 것, 및

상기 S-박스 출력 값을 생성하기 위해 상기 제 1 중간 값 및 상기 제 1 값에 대해 비트와이즈 XOR 동작을 수행하는 것, 또는

(C) 상기 제 1 중간 값을 생성하기 위해 상기 입력 값 및 상기 제 1 값에 대해 비트와이즈 XOR 동작을 수행하는 것,

제 2 중간 값을 생성하기 위해 상기 제 1 중간 값의 해밍 웨이트와 동일한 비트들의 수 만큼 상기 제 1 중간 값에 대해 비트와이즈 회전 동작을 수행하는 것,

제 2 값을 획득하는 것, 및

상기 S-박스 출력 값을 생성하기 위해 상기 제 2 중간 값 및 상기 제 2 값에 대해 비트와이즈 XOR 동작을 수행하는 것,

중 하나에 의해, S-박스 출력 값을 생성하게 하는,

컴퓨터-판독 가능한 저장 매체.

청구항 26

제 25 항에 있어서,

제공된 상기 제 1 값 및/또는 제 2 값 중 적어도 하나는 50%와 같거나 그 초과의 확률로 상기 입력 값과 상이한 해밍 웨이트를 갖는 S-박스 출력 값을 생성하도록 구성되는,

컴퓨터-판독 가능한 저장 매체.

청구항 27

제 25 항에 있어서,

상기 제 1 값 및/또는 상기 제 2 값 중 적어도 하나는 비-제로(non-zero) 해밍 웨이트를 갖는 상수인,

컴퓨터-판독 가능한 저장 매체.

청구항 28

제 25 항에 있어서,

상기 명령들은, 상기 프로세서에 의해 실행될 때, 상기 프로세서로 하여금 추가로,

메인 입력 값을 획득하게 하고;

복수의 NLTF(non-linear transformation function) 입력 값들을 획득하도록 상기 메인 입력 값의 비트들을 배분하게 하고 - 각각의 NLTF 입력 값은 상기 메인 입력 값의 비트들의 수 미만인 비트들의 수를 가짐 - ;

상기 NLTF에 제공되는 NLTF 입력 값에 각각 대응하는 복수의 NLTF 출력 값들을 생성하도록 비-선형 동작을 실행하는 NLTF에 상기 NLTF 입력 값들 각각을 제공하게 하고; 및

상기 입력 값을 획득하도록 상기 복수의 NLTF 출력 값들을 연계하게 하는

컴퓨터-판독 가능한 저장 매체.

발명의 설명

기 술 분 야

[0001] 우선권 주장

[0002] [0001] 본 특허 출원은 2013년 1월 11일 출원되고 발명의 명칭이 "Method and Apparatus for Computable,

Large, Variable, and Secure Substitution Box"인 가출원 번호 제61/751,541호를 우선권으로 주장하며, 상기 가출원의 전체 개시물은 그에 의해 명시적으로 인용에 의해 포함된다.

[0003] [0002] 다양한 특징들은 암호법(cryptography)에 관한 것으로서, 보다 구체적으로는, 치환-박스들(Substitution-boxes)을 구현하기 위한 방법들 및 장치들에 관한 것이다.

배 경 기 술

[0004] [0003] 암호법에서, S-박스(Substitution-box)는 치환을 수행하는 대칭키 알고리즘의 기본 컴포넌트이다. 블록 암호들에서, 이들은 통상적으로 키와 암호-텍스트 간의 관계를 모호하게 하고 이에 따라 섀넌의 혼란 특성(Shannon's property of confusion)을 나타내도록 이용된다. S-박스는, 출력이 특정한 암호적으로 유용한 특성들을 갖도록 n개의 입력 비트들을 수신하고 m개의 출력 비트들을 생성하는 복합 기능을 나타낸다. 이들 특성들은 높은 비-선형성 및 밸런스, 높은 대수적 정도(algebraic degree), 엄격한 애벌런시(avalanche) 기준 만족 및 다른 특성들을 포함한다. 이러한 기능들은 컴퓨팅하기 어렵고, 종종 DES(Data Encryption Standard) 및 AES(Advanced Encryption Standard)에서와 같이 룩업 테이블들로서 표현된다. 예를 들어, AES에서, 8-비트 입력은 S-박스로부터 선택된 8-비트 값으로 대체된다. 몇몇 경우들에서, S-박스에 대한 입력 및 출력이 동일한 비트 길이들을 갖도록 n은 m과 동일할 수 있다.

[0005] [0004] n이 큰 경우, 위에서 설명된 룩업 테이블들(또는 등가로, 하드웨어 구현을 위한 게이트들의 네트워크)은 빠르게 너무 커질 수 있다. 한편, 작은 n은 정의에 의해 비선형성 및 대수학 정도에서 제한된다. 그러므로, 하드웨어 또는 소프트웨어에서 효율적으로 구현될 수도 있는 매우 다수의 입력 비트들을 갖는 S-박스가 바람직하다.

[0006] [0005] HWBF(Hidden Weighted Bit Function)는 밸런스 및 대수학 복잡도와 같이 위에서 설명된 바람직한 암호 특성들 중 일부를 향유하는 n-비트 대 1-비트 S 박스로서 고려될 수 있다. 예를 들어, x가 n-비트 입력인 경우 (x_i는 x의 i-번째(1 <= i <= n)의 최상위 비트임), HWBF의 출력 W는 다음과 같이 정의된다:

[0007] x = 0인 경우, W(x) = 0이고,

[0008] 그렇지 않으면, $W(x) = x_k$ 이며, 여기서 k는 x의 해밍 웨이트(Hamming Weight)이다.

[0009] [0006] 도 1은 하드웨어로 쉽게 구현될 수 있는, 종래 기술에서 발견된 n-비트 대 n-비트 HWBF 기반 S-박스(100)의 개략적 블록도를 예시한다. 이진 입력 값 x(예를 들어, 110101)는 회전 함수(102)에 입력된다. 회전 함수(102)는 입력의 해밍 웨이트와 동일한 비트들의 수만큼 입력 x 상에서 좌측으로 비트와이즈 회전(bitwise rotation)을 수행한다. 따라서, 이진 입력 x가 110101과 동일한 경우, 회전 함수(102)의 출력 z는 해밍 웨이트가 넷(4)과 동일하므로 011101과 동일하다.

[0010] [0007] 도 2는 HWBF 기반 S-박스 출력 z와 HWBF W(x) 간의 관계를 도시하는 표(200)를 예시한다. 도 1 및 도 2를 참조하면, 출력 z(예를 들어, 1)의 최하위 비트가 입력 값 x의 HWBF W(x)(위에서 정의됨)와 동일하다는 것이 도시될 수 있다. 또한, 제 2 최하위 비트(예를 들어, 0)는 HWBF에 대한 입력 값(x)이 우측으로 1 비트 비트와이즈 회전(W(x<<1로 표시됨)을 경험한 경우 HWBF W(x)의 출력을 나타낸다는 것이 관찰될 수 있다. 제 3 최하위 비트는, HWBF에 대한 입력 값(x)이 우측으로 2비트 비트와이즈 회전(W(x<<2)로 표시됨)을 경험한 경우 HWBF W(x)의 출력을 나타내는 식이다.

[0011] [0008] 따라서, 출력 값(z)은 입력 값(x)과 동일한 수의 비트들을 가지며, 여기서 각각의 비트는 병렬로 컴퓨팅되는 상이한 HWBF W(x) 출력을 나타낸다. 출력 값(z)의 비트들은 HWBF들에 관하여 위에서 설명된 유리한 암호 특성들 중 일부를 여전히 보유한다. 불행히도, S-박스(100)는 또한 바람직하지 않은 특성들도 갖는다. 예를 들어, 하나의 이러한 바람직하지 않은 특성은, 출력(z)이 입력(x)과 동일한 해밍 웨이트를 가질 것이란 것이며, 이는 종종, 특히 입력(x)이 낮은 해밍 웨이트를 가질 때 암호해독(cryptanalysis)을 단순하게 할 수 있다. 암호 공격들(암호해독)에 보다 더 저항력이 있게 하기 위해 S-박스(100)의 보안을 증가시키는 것이 바람직할 것이다.

[0012] [0009] 따라서, 암호 공격들에 대하여 보다 더 강건한 개선된 S-박스 알고리즘, 방법들 및 장치들이 필요하다.

발명의 내용

[0013] [0010] 하나의 특징은 S-박스(substitution box)와 연관되는 암호 값들을 생성하기 위한 방법을 제공한다. 이 방법은 입력 값 및 제 1 값을 획득하는 단계; 및 (A) 제 1 중간 값을 생성하기 위해 입력 값 및 제 1 값에 대

해 비트와이즈 배타적 OR(XOR) 동작을 수행하는 것, 및 S-박스 출력 값을 생성하기 위해 제 1 중간 값의 해밍 웨이트(Hamming Weight)와 동일한 비트들의 수 만큼 제 1 중간 값에 대해 비트와이즈 회전 동작을 수행하는 것; (B) 제 1 중간 값을 생성하기 위해 입력 값의 해밍 웨이트와 동일한 비트들의 수 만큼 입력 값에 대해 비트와이즈 회전 동작을 수행하는 것, 및 S-박스 출력 값을 생성하기 위해 제 1 중간 값 및 제 1 값에 대해 비트와이즈 XOR 동작을 수행하는 것, 또는 (C) 제 1 중간 값을 생성하기 위해 입력 값 및 제 1 값에 대해 비트와이즈 XOR 동작을 수행하는 것, 제 2 중간 값을 생성하기 위해 제 1 중간 값의 해밍 웨이트와 동일한 비트들의 수 만큼 제 1 중간 값에 대해 비트와이즈 회전 동작을 수행하는 것, 제 2 값을 획득하는 것, 및 S-박스 출력 값을 생성하기 위해 제 2 중간 값 및 제 2 값에 대해 비트와이즈 XOR 동작을 수행하는 것 중 하나에 의해 S-박스 출력 값을 생성하는 단계를 포함한다. 일 양상에 따라, 제공된 제 1 값 및/또는 제 2 값 중 적어도 하나는 50%와 같거나 그 초과의 확률로 입력 값과 상이한 해밍 웨이트를 갖는 S-박스 출력 값을 생성하도록 구성된다. 다른 양상에 따라, 제 1 값 및/또는 제 2 값 중 적어도 하나는 비-제로(non-zero) 해밍 웨이트를 갖는 상수이다.

[0014] [0011] 일 양상에 따라, 제공된 제 1 값 및/또는 제 2 값 중 적어도 하나는 가변적이고 $100*(1-2^{-n})$ 퍼센트와 같거나 그 초과의, 비-제로 해밍 웨이트를 가질 확률을 가지며, 여기서 n은 제 1 값 및/또는 제 2 값의 비트들의 수이다. 다른 양상에 따라, 제 1 값 및/또는 제 2 값 중 적어도 하나는 암호 함수 및/또는 암호 키 중 적어도 하나로부터 유도된다. 또 다른 양상에 따라, 제 1 값 및/또는 제 2 값 중 적어도 하나는 암호 모듈의 컴포넌트 스테이지로부터 유도된다.

[0015] [0012] 일 양상에 따라, 암호 모듈은 스트림 암호이다. 다른 양상에 따라, 이 방법은 메모리 회로에서 실행된다. 또 다른 양상에 따라, 입력 값 및 S-박스 출력 값은 동일한 비트들의 수를 갖는다.

[0016] [0013] 일 양상에 따라, 이 방법은 메인 입력 값을 획득하는 단계; 복수의 NLTF(non-linear transformation function) 입력 값들을 획득하도록 메인 입력 값의 비트들을 배분하는 단계 - 각각의 NLTF 입력 값은 메인 입력 값의 비트들의 수 미만인 비트들의 수를 가짐 - ; NLTF에 제공되는 NLTF 입력 값에 각각 대응하는 복수의 NLTF 출력 값들을 생성하도록 비-선형 동작을 실행하는 NLTF에 NLTF 입력 값들 각각을 제공하는 단계; 및 입력 값을 획득하도록 복수의 NLTF 출력 값들을 연계(concatenating)하는 단계를 더 포함한다. 다른 양상에 따라, 메인 입력 값은 복수의 NLTF 입력 값들 각각이 동일한 비트들의 수를 갖도록 배분된다.

[0017] [0014] 다른 특징은 프로세싱 회로를 포함하는 전자 디바이스를 제공하며, 이 프로세싱 회로는 입력 값 및 제 1 값을 획득하도록; 그리고 (A) 제 1 중간 값을 생성하기 위해 입력 값 및 제 1 값에 대해 비트와이즈 배타적 OR(XOR) 동작을 수행하는 것, 및 S-박스 출력 값을 생성하기 위해 제 1 중간 값의 해밍 웨이트(Hamming Weight)와 동일한 비트들의 수 만큼 제 1 중간 값에 대해 비트와이즈 회전 동작을 수행하는 것; (B) 제 1 중간 값을 생성하기 위해 입력 값의 해밍 웨이트와 동일한 비트들의 수 만큼 입력 값에 대해 비트와이즈 회전 동작을 수행하는 것, 및 S-박스 출력 값을 생성하기 위해 제 1 중간 값 및 제 1 값에 대해 비트와이즈 XOR 동작을 수행하는 것, 또는 (C) 제 1 중간 값을 생성하기 위해 입력 값 및 제 1 값에 대해 비트와이즈 XOR 동작을 수행하는 것, 제 2 중간 값을 생성하기 위해 제 1 중간 값의 해밍 웨이트와 동일한 비트들의 수 만큼 제 1 중간 값에 대해 비트와이즈 회전 동작을 수행하는 것, 제 2 값을 획득하는 것, 및 S-박스 출력 값을 생성하기 위해 제 2 중간 값 및 제 2 값에 대해 비트와이즈 XOR 동작을 수행하는 것 중 하나에 의해 S-박스 출력 값을 생성하도록 구성된다.

[0018] [0015] 일 양상에 따라, 프로세싱 회로는 추가로, 메인 입력 값을 획득하도록; 복수의 NLTF(non-linear transformation function) 입력 값들을 획득하도록 메인 입력 값의 비트들을 배분하도록 - 각각의 NLTF 입력 값은 메인 입력 값의 비트들의 수 미만인 비트들의 수를 가짐 - ; NLTF에 제공되는 NLTF 입력 값에 각각 대응하는 복수의 NLTF 출력 값들을 생성하도록 비-선형 동작을 실행하는 NLTF에 NLTF 입력 값들 각각을 제공하도록; 그리고 입력 값을 획득하도록 복수의 NLTF 출력 값들을 연계하도록 구성된다.

[0019] [0016] 다른 특징은 전자 디바이스를 제공하며, 이 전자 디바이스는, 입력 값 및 제 1 값을 획득하기 위한 수단; 및 (A) 제 1 중간 값을 생성하기 위해 입력 값 및 제 1 값에 대해 비트와이즈 배타적 OR(XOR) 동작을 수행하기 위한 수단, 및 S-박스 출력 값을 생성하기 위해 제 1 중간 값의 해밍 웨이트(Hamming Weight)와 동일한 비트들의 수 만큼 제 1 중간 값에 대해 비트와이즈 회전 동작을 수행하기 위한 수단; (B) 제 1 중간 값을 생성하기 위해 입력 값의 해밍 웨이트와 동일한 비트들의 수 만큼 입력 값에 대해 비트와이즈 회전 동작을 수행하기 위한 수단, 및 S-박스 출력 값을 생성하기 위해 제 1 중간 값 및 제 1 값에 대해 비트와이즈 XOR 동작을 수행하기 위한 수단, 또는 (C) 제 1 중간 값을 생성하기 위해 입력 값 및 제 1 값에 대해 비트와이즈 XOR 동작을 수행하기 위한 수단, 제 2 중간 값을 생성하기 위해 제 1 중간 값의 해밍 웨이트와 동일한 비트들의 수 만큼 제 1 중간 값에 대해 비트와이즈 회전 동작을 수행하기 위한 수단, 제 2 값을 획득하기 위한 수단, 및 S-박스 출력

값을 생성하기 위해 제 2 중간 값 및 제 2 값에 대해 비트와이즈 XOR 동작을 수행하기 위한 수단 중 하나에 의해 S-박스 출력 값을 생성하기 위한 수단을 포함한다.

[0020] [0017] 일 양상에 따라, 전자 디바이스는 메인 입력 값을 획득하기 위한 수단; 복수의 NLTF(non-linear transformation function) 입력 값들을 획득하기 위해 메인 입력 값의 비트들을 배분하기 위한 수단 - 각각의 NLTF 입력 값은 메인 입력 값의 비트들의 수 미만인 비트들의 수를 가짐 - ; NLTF에 제공되는 NLTF 입력 값에 각각 대응하는 복수의 NLTF 출력 값들을 생성하기 위해 비-선형 동작을 실행하는 NLTF에 NLTF 입력 값들 각각을 제공하기 위한 수단; 및 입력 값을 획득하기 위해 복수의 NLTF 출력 값들을 연계하기 위한 수단을 더 포함한다.

[0021] [0018] 다른 특징은 S-박스(substitution box)와 연관된 암호 값을 생성하기 위한 명령들이 저장되어 있는 컴퓨터-판독 가능한 저장 매체를 제공하며, 명령은 적어도 하나의 프로세서에 의해 실행될 때, 프로세서로 하여금, 입력 값 및 제 1 값을 획득하게 하고, 그리고 (A) 제 1 중간 값을 생성하기 위해 입력 값 및 제 1 값에 대해 비트와이즈 배타적 OR(XOR) 동작을 수행하는 것, 및 S-박스 출력 값을 생성하기 위해 제 1 중간 값의 해밍 웨이트(Hamming Weight)와 동일한 비트들의 수 만큼 제 1 중간 값에 대해 비트와이즈 회전 동작을 수행하는 것; (B) 제 1 중간 값을 생성하기 위해 입력 값의 해밍 웨이트와 동일한 비트들의 수 만큼 입력 값에 대해 비트와이즈 회전 동작을 수행하는 것, 및 S-박스 출력 값을 생성하기 위해 제 1 중간 값 및 제 1 값에 대해 비트와이즈 XOR 동작을 수행하는 것, 또는 (C) 제 1 중간 값을 생성하기 위해 입력 값 및 제 1 값에 대해 비트와이즈 XOR 동작을 수행하는 것, 제 2 중간 값을 생성하기 위해 제 1 중간 값의 해밍 웨이트와 동일한 비트들의 수 만큼 제 1 중간 값에 대해 비트와이즈 회전 동작을 수행하는 것, 제 2 값을 획득하는 것, 및 S-박스 출력 값을 생성하기 위해 제 2 중간 값 및 제 2 값에 대해 비트와이즈 XOR 동작을 수행하는 것 중 하나에 의해 S-박스 출력 값을 생성하게 한다.

[0022] [0019] 일 양상에 따라, 이 명령들은, 프로세서에 의해 실행될 때, 프로세서로 하여금 추가로, 메인 입력 값을 획득하게 하고; 복수의 NLTF(non-linear transformation function) 입력 값들을 획득하도록 메인 입력 값의 비트들을 배분하게 하고 - 각각의 NLTF 입력 값은 메인 입력 값의 비트들의 수 미만인 비트들의 수를 가짐 - ; NLTF에 제공되는 NLTF 입력 값에 각각 대응하는 복수의 NLTF 출력 값들을 생성하도록 비-선형 동작을 실행하는 NLTF에 NLTF 입력 값들 각각을 제공하게 하고; 및 입력 값을 획득하도록 복수의 NLTF 출력 값들을 연계하게 한다.

도면의 간단한 설명

[0023] [0020] 도 1은 종래 기술에서 발견되는 n-비트 대 n-비트 HWBF(Hamming Weighted Bit Function) 기반 S-박스(substitution box)의 개략적 블록도를 예시한다.

[0021] 도 2는 HWBF 기반 S-박스 출력(z)과 HWBF W(x) 간의 관계를 도시하는 표를 예시한다.

[0022] 도 3은 S-박스의 제 1 예시적인 개략적 블록도를 예시한다.

[0023] 도 4는 S-박스의 제 2 예시적인 개략적 블록도를 예시한다.

[0024] 도 5는 S-박스의 제 3 예시적인 개략적 블록도를 예시한다.

[0025] 도 6은 암호 함수(f)가 암호 키/식별자(K1)로부터 가변 값(C1)을 유도하는 예를 예시한다.

[0026] 도 7은 가변 값(C2)이 암호 모듈의 스테이지로부터 유도/수신되는 예를 예시한다.

[0027] 도 8은 S-박스의 제 4 예시적인 개략적 블록도를 예시한다.

[0028] 도 9는 S-박스와 연관된 암호 값들을 생성하는 방법의 흐름도를 예시한다.

[0029] 도 10은 본 명세서에서 설명되는 S-박스를 포함하는 전자 디바이스에 대한 하드웨어 구현의 개략적 블록도를 예시한다.

[0030] 도 11은 전자 디바이스의 프로세서의 개략적 블록도를 예시한다.

발명을 실시하기 위한 구체적인 내용

[0024] [0031] 다음의 설명에서, 특정한 세부사항들은 본 개시의 다양한 양상들의 완전한 이해를 제공하기 위해 주어진다. 그러나 양상들은 이들 특정한 세부사항들 없이 실시될 수 있다는 것이 당업자에 의해 이해될 것이다. 예를 들어, 회로들은 불필요한 세부사항들로 양상들을 모호하게 하는 것을 방지하기 위해 블록도들로 도시될 수

있다. 다른 인스턴스들에서, 잘-알려진 회로들, 구조들 및 기법들은 본 개시의 양상들을 모호하게 하지 않도록 상세히 도시되지 않을 수 있다.

[0025] [0032] "예시적인"이란 단어는 "예, 보기, 또는 예시로서 작용하는 것"을 의미하도록 본 명세서에서 이용된다. "예시적인" 것으로서 본 명세서에서 설명되는 임의의 구현 또는 양상은 반드시 본 개시의 다른 양상들보다 선호되거나 유리한 것으로서 해석될 필요는 없다. 마찬가지로, "양상들"이란 용어는 본 개시의 모든 양상들이 논의된 특징, 이점 또는 동작 모드를 포함할 것을 요구하는 것은 아니다.

[0026]

[0027] **예시적인 S-박스 : HWBF의 입력 상에서 수행되는 XOR(Exclusive OR) 동작**

[0028] [0033] 도 3은 본 개시의 일 양상에 따른 S-박스(300)의 개략적 블록도를 예시한다. 비트와이즈 배타적 OR(XOR) 함수(302)는 입력들로서 입력 값(x)(예를 들어, 110101) 및 제 1 값(예를 들어, 100110)을 수신한다. 예시된 예에서, 제 1 값은 비-제로 해밍 웨이트를 갖는 상수값이다. 비트와이즈 XOR 함수(302)는 회전 함수(304)내로 입력되는 제 1 중간 출력(y)(예를 들어, 010011)을 생성한다. 이 예에서, 회전 함수(304)는 출력(y)의 해밍 웨이트만큼 제 1 중간 출력 상에서 좌측으로 비트와이즈 회전(예를 들어, 3만큼 좌측으로 회전)을 수행한다. 회전 함수(304)의 결과적인 출력(z)(예를 들어, 011010)은 n 병렬 HWBF 출력들을 나타내며, 여기서 n은 입력 값(x)의 비트-길이이다. 명백히, 출력(z)은 입력 값(x)과 동일한 해밍 웨이트를 반드시 가질 필요는 없고, 이에 따라 S-박스(300)의 출력(z)은 종래 기술의 방법들보다 암호해독에 대해 더 안전하다. S-박스(300)의 출력(z)은 입력(x)과 동일한 수의 비트들을 가질 수 있다. 일 양상에 따라, 회전 함수(304)는 우측으로 비트와이즈 회전을 대신 수행할 수 있으며, 이 프로세스는 여전히 암호 보안의 견지에서 등가일 것이다.

[0029] [0034] XOR 함수(302)는 제 1 중간 값을 생성하기 위해 제 1 값 및 입력 값에 대해 비트와이즈 배타적 OR 동작을 수행하기 위한 수단의 일 예로서의 역할을 하는 XOR 회로일 수 있다. 회전 함수(304)는 S-박스 출력 값을 생성하기 위해 제 1 중간 값의 해밍 웨이트와 동일한 비트들의 수만큼 제 1 중간 값에 대해 비트와이즈 회전 동작을 수행하기 위한 수단; 및 출력 S-박스 값을 생성하기 위한 수단의 일 예로서의 역할을 하는 회전 $\text{Rotate}_{\text{HM}}$ 회로에 의해 실행될 수 있다.

[0030] **예시적인 S-박스: HWBF의 출력 상에서 수행되는 XOR 동작**

[0031] [0035] 도 4는 본 개시의 일 양상에 따라 S-박스(400)의 개략적 블록도를 예시한다. 회전 함수(402)는 입력으로서 입력 값(x)(예를 들어, 110101)을 수신한다. 이 예에서, 회전 함수(402)는 입력(x)의 해밍 웨이트 만큼 입력 값에 대해 좌측으로 비트와이즈 회전(예를 들어, 4만큼 좌측으로 회전)을 수행하여 제 1 중간 출력(y)(예를 들어, 011101)을 생성한다. 회전 함수(402)의 결과적인 중간 출력(y)은 n 병렬 HWBF 출력들을 나타내며, 여기서 n은 입력 값(x)의 비트-길이이다. 다음으로, 비트와이즈 XOR 함수(404)는 입력들로서 중간 출력(y) 및 제 1 값(예를 들어, 101100)을 수신한다. 이 예시된 예에서, 제 1 값은 비-제로 해밍 웨이트를 갖는 상수값이다. XOR 함수(404)는 입력 값(x)과 동일한 해밍 웨이트를 반드시 가질 필요는 없는 출력(z)(예를 들어, 110001)을 생성한다. 따라서, S-박스(400)의 출력(z)은 종래 기술의 방법들보다 암호해독에 대해 더 안전하다. S-박스(400)의 출력(z)은 입력(x)과 동일한 수의 비트들을 가질 수 있다. 일 양상에 따라 회전 함수(402)는 우측으로 비트와이즈 회전을 대신 수행할 수 있고, 이 프로세스는 여전히 암호 보안의 견지에서 등가일 것이다.

[0032] [0036] 회전 함수(402)는 제 1 중간 값을 생성하기 위해 입력 값의 해밍 웨이트와 동일한 비트들의 수 만큼 입력 값에 대해 비트와이즈 회전 동작을 수행하기 위한 수단의 일 예로서의 역할을 하는 $\text{Rotate}_{\text{HM}}$ 회로에 의해 실행될 수 있다. XOR 함수(404)는 S-박스 출력 값을 생성하기 위해 제 1 값 및 제 1 중간 값에 대해 비트와이즈 XOR 동작을 수행하기 위한 수단; 및 출력 S-박스 값을 생성하기 위한 수단의 일 예로서의 역할을 하는 XOR 회로에 의해 실행될 수 있다.

[0033] **예시적인 S-박스: HWBF의 입력 및 출력에서 수행되는 XOR 동작**

[0034] [0037] 도 5는 본 개시의 일 양상에 따른 S-박스(500)의 개략적 블록도를 예시한다. 비트와이즈 XOR 함수(502)는 입력들로서 입력 값(x)(예를 들어, 110101) 및 제 1 값(예를 들어, 001100)을 수신한다. 예시된 예에서, 제 1 입력 값은 비-제로 해밍 웨이트를 갖는 상수값이다. 비트와이즈 XOR 함수(502)는 회전 함수(504)에 입력되는 제 1 중간 출력(w)(예를 들어, 111001)을 생성한다. 이 예에서, 회전 함수(504)는 출력(w)의 해밍 웨이트 만큼 제 1 중간 출력(w) 상에서 좌측으로 비트와이즈 회전(예를 들어, 4만큼 좌측으로 회전)을 수행한다. 회전 함수(504)의 결과적인 제 2 중간 출력(y)(예를 들어, 011110)은 n 병렬 HWBF 출력들을 나타내며, 여기서 n은 중간

값(y)의 비트-길이이다. 그 후, 다른 비트와이즈 XOR 함수(506)는 입력들로서 제 2 중간 출력(y) 및 제 2 값(예를 들어, 111000)을 수신한다. 예시된 예에서, 제 2 값은 비-제로 해밍 웨이트를 갖는 상수값이다. XOR 함수(506)는 입력 값(x)과 동일한 해밍 웨이트를 반드시 가질 필요는 없는 출력(z)(예를 들어, 100110)을 생성한다. 따라서, S-박스(500)의 출력(z)은 종래 기술의 방법들보다 암호해독에 대해 더 안전하다. S-박스(500)의 출력(z)은 입력(x)과 동일한 수의 비트들을 가질 수 있다. 일 양상에 따라, 회전 함수(504)는 우측으로 비트와이즈 회전을 대신 수행할 수 있고, 이 프로세스는 여전히 암호 보안의 견지에서 등가일 것이다.

[0035] [0038] XOR 함수(502)는 제 1 중간 값을 생성하기 위해 입력 값 및 제 1 값에 대해 비트와이즈 XOR 동작을 수행하기 위한 수단의 일 예로서의 역할을 하는 XOR 회로에 의해 실행될 수 있다. 회전 함수(504)는 제 2 중간 값을 생성하기 위해 제 1 중간 값의 해밍 웨이트와 동일한 비트들의 수 만큼 제 1 중간 값에 대해 비트와이즈 회전 동작을 수행하기 위한 수단의 일 예로서의 역할을 하는 $Rotate_{HM}$ 회로에 의해 실행될 수 있다. XOR 함수(506)는 S-박스 출력 값을 생성하기 위해 제 2 중간 값 및 제 2 값에 대해 비트와이즈 XOR 동작을 수행하기 위한 수단; 및 출력 S-박스 값을 생성하기 위한 수단의 일 예로서의 역할을 하는 XOR 회로에 의해 실행될 수 있다.

[0036] [0039] 도 3, 도 4 및 도 5에 관하여 위에서 설명된 예들에서, 회전 함수들은 그의 입력의 해밍 웨이트와 동일하게 좌측으로 비트와이즈 회전을 수행한다. 그러나 다른 양상들에서 회전 함수들은 그의 입력의 해밍 웨이트와 동일하게 우측으로 비트와이즈 회전을 수행할 수 있다. 이러한 경우에, 회전 함수에 의해 출력된 값의 최상위 비트(최하위 비트 대신)는 대안적인 HWBF W'(x)의 출력을 나타낸다. 대안적인 HWBF W'(x)는 n-비트 입력인 입력 x를 가질 수 있으며 여기서 x_i는 x의 i-번째($1 <= i <= n$)의 최하위 비트이다. 따라서 함수 W'(x)는 다음과 같이 정의된다:

[0037] x = 0인 경우, W'(x) = 0이고,

[0038] 그렇지 않으면, $W'(x) = x_k$ 이며, 여기서 k는 x의 해밍 웨이트이다.

[0039] [0040] 일 예로서, 회전 함수(504)가 좌측 대신 우측으로 제 1 중간 값(w)(111001)을 회전시킨 경우, 제 2 중간 값(y)은 011110 대신 100111와 동일할 것이다. 제 2 값(111000)과의 XOR 연산(506) 이후에, S-박스(500)의 출력(z)은 011111일 것이다.

[0040] [0041] 일 양상에 따라, XOR 함수들(302, 404, 502, 506)에 입력된 제 1 값 및 제 2 값은 위에서 설명된 바와 같은 상수들일 수 있다. 그러나 다른 양상들에서, 제 1 값 및 제 2 값은 전혀 상수일 필요는 없다. 일 양상에서, 제 1 값 및 제 2 값은 적시에, 시동시에 그리고/또는 S-박스들(300, 400, 500)의 특정한 횟수의 반복들(즉, 출력 값들이 생성됨) 이후에 그의 값들의 변하도록 가변 가능할 수 있다. 일 예로서, 제 1 값 및 제 2 값은, 이들이 변경되는 함수를 이용하여 암호 키로부터 유도되거나 키 그 자체가 변경된다는 점에서 가변적일 수 있다. 이러한 방식은 S-박스들(300, 400, 500)의 출력을 암호 공격들에 대해 보다 강건하게 할 수 있다. 일 양상에 따라, 제공되는 제 1 값 및/또는 제 2 값은 50%와 같거나 그 초과의 확률로 입력 값과 상이한 해밍 웨이트를 갖는 S-박스 출력 값들을 생성하도록 구성된다.

[0041] **제 1 값 및 제 2 값의 예시적인 타입들**

[0042] [0042] 도 6은 암호 함수(f)(602)가 암호 키/식별자(K_1)로부터 가변 값(C_1)을 유도하는 하나의 이러한 예를 예시한다. 암호 함수(f)(602)는 다른 것들 중에서도, 해시 함수일 수 있다. 가변 값(C_1)은 이어서, 도 3을 참조하여 위에서 설명된 바로 그 방식으로 XOR 함수(302)에 입력된 제 1 값으로서 이용되어서 S-박스(300) 출력(z)을 생성한다. 다른 S-박스들(400, 500) 중 임의의 것은, 그 내부에서 이용되는 제 1 값 및/또는 제 2 값은 암호 함수(f)(602) 및/또는 키/식별자(K_1)와 같은 암호 함수들을 이용하여 키들/식별자들로부터 유도되도록, 동일한 방식으로 변형될 수 있다.

[0043] [0043] 제 1 값 및 제 2 값이 가변적인 다른 양상에 따라, 제 1 값 및 제 2 값은 S-박스 부근에서 발생하는 암호의 다른 동작들로부터 유도될 수 있다. 도 7은 가변 값(C_2)이 암호 모듈(702)의 스테이지로부터 유도/수신되는 하나의 이러한 예를 예시한다. 암호 모듈(702)은 복수의 N 정수 컴포넌트들(704, 706, 708)을 포함할 수 있고, 가변 값(C_2)은 이들 컴포넌트들(704, 706, 708) 중 임의의 하나에 대한 입력 또는 출력으로부터 유도될 수 있다. 컴포넌트들(704, 706, 708)은 다른 것들 중에서도, 시프트 레지스터들, 덧셈기들, 곱셈기들, 프로세싱 회로들/블록들 등일 수 있다. 일 양상에서, S-박스들(300, 400, 500)은 암호 모듈(702)의 부분일 수 있지만, 다른 양상들에서, S-박스들(300, 400, 500)은 암호 모듈(702)에 독립적일 수 있다. 일 예에 따라, 암호 블록(702)은

스트림 암호일 수 있다.

[0044] [0044] 가변 값(C2)은 이어서 도 3을 참조하여 위에서 설명된 바로 그 방식으로 XOR 함수(302)에 입력된 제 1 값으로서 이용되어서 S-박스 (300) 출력(z)을 생성한다. 다른 S-박스들(400, 500) 중 임의의 것은, 그 내부에서 이용되는 제 1 값 및/또는 제 2 값은 도 7에서 도시된 암호 모듈의 하나 또는 그 초과의 스테이지들로부터 유도되도록, 동일한 방식으로 변형될 수 있다.

[0045] [0045] 일 양상에 따라, 가변 입력들(C_1 및 C_2)(즉, 제 1 값 및 제 2 값)은 이들이 50%, 60%, 70%, 80%, 90%, 95%, 또는 99% 중 하나와 동일하거나 이보다 더 큰, 비-제로 해밍 웨이트를 가질 확률을 갖도록 제공될 수 있다. 다른 양상에 따라, 가변 입력들(C_1 및 C_2)은 이들이 $100*(1-2^{-n})$ 퍼센트와 동일하거나 더 큰, 비-제로 해밍 웨이트를 가질 확률을 갖도록 제공될 수 있으며, 여기서 n은 가변 입력들(C_1 및 C_2)의 비트들의 수이다.

[0046] **부가적인 NLTF 스테이지들을 특징으로 하는 예시적인 S-박스**

[0047] [0046] 도 8은 본 개시의 다른 양상에 따라 S-박스(800)의 개략적 블록도를 예시한다. S-박스(800)(예를 들어, "메인 S-박스")는 비트 배분 회로(802), 복수(N)의 NLTF(non-linear transformation functions) 서브-회로들(804, 806, 808, 810)(여기서 N은 둘(2) 또는 그 초과의 정수임), 연계 회로(812), 및 S-박스 A 서브-회로(814)를 포함한다. 비(non) NLTF 서브-회로들(804, 806, 808, 810)은 표준 비-선형 변환 테이블-기반 S-박스들일 수 있다. S-박스 서브-회로 A(814)는 도 3 내지 도 7에서 도시되고 설명된 S-박스들(300, 400, 500) 중 임의의 하나이다.

[0048] [0047] 메인 S-박스(800)는 n-비트 메인 입력(x)을 수신하고, 암호 보안을 개선하는 n-비트 메인 S-박스 출력(z)을 생성한다. 비트 배분 회로(802)는 n-비트 메인 입력(x)을 복수의 더 작은 m_1, m_2, m_3,… m_N 비트 NLTF 입력 값들(803a, 803b, 803c, … 803n)로 분해한다(즉, m_1, m_2, m_3,… m_N 은 n 미만임). 비 NLTF 서브-회로들(804, 806, 808, 810)은 비-선형 동작에 따라 NLTF 입력 값들(803a, 803b, 803c, … 803n)을 NLTF 출력 값들(805a, 805b, 805c, … 805n)로 변환하기 위해 룩업 테이블들을 이용할 수 있다. NLTF 입력 값들(803a, 803b, 803c,… 803n)은 그의 대응하는 NLTF 출력 값들(805a, 805b, 805c, … 805n)과 동일한 수의 비트들을 가질 수 있다. NLTF 출력 값들(805a, 805b, 805c, … 805n)은 이어서 n-비트 입력 값(y)을 생성하기 위해 연계 회로(812)에 의해 함께 연계된다. 도 3 내지 도 7에 관하여 위에서 설명된 동작들/단계들과 동일하게, S-박스 A(804)는 제 1 및/또는 제 2 값(예를 들어, 도 3 내지 도 7 참조)과 함께 n-비트 입력 값(y)을 수신하고 메인 n-비트 S-박스 출력 값(z)을 생성하기 위해 하나 또는 그 초과의 XOR 및 해밍 웨이트 회전 동작들(예를 들어, 도 3 내지 도 7 참조)을 수행한다. 이들 출력 값들은 S-박스 서브-회로들(804, 806, 808, 810)에 의해 수신된 입력 값들과 동일한 비트 길이(즉, m_1, m_2, m_3, 및 m_N)를 가질 수 있다.

[0049] [0048] 일 양상에 따라, 비트 배분 회로(802)는 복수의 NLTF(non-linear transformation function) 입력 값들을 획득하기 위해 메인 입력 값의 비트들을 배분하기 위한 수단의 일 예로서의 역할을 하며, 여기서 각각의 NLTF 입력 값은 메인 입력 값의 비트들의 수보다 작은 비트들의 수를 갖는다. 비트 배분 회로(802)는 NLTF에 제공된 NLTF 입력 값에 각각 대응하는 복수의 NLTF 출력 값들을 생성하기 위해 비-선형 동작을 실행하는 NLTF에 각각의 NLTF 입력 값들을 제공하기 위한 수단의 일 예로서 또한 역할을 한다. 연계 회로(812)는 입력 값을 획득하기 위해 복수의 NLTF 출력 값들을 연계하기 위한 수단의 일 예로서의 역할을 한다.

[0050] [0049] 메인 S-박스(800)의 동작이 이제 하나의 비-제한적인 예에 따라 설명될 것이다. 메인 S-박스(800)는 비트들(b_0, b_1, b_2, … b_{31})을 갖는 32-비트 메인 입력(x)을 수신할 수 있고 이 32-비트 메인 입력(x)을 비트 배분 회로(802)가 NLTF 서브-회로들(804, 806, 808, 810)에 대한 넷(4)의 8-비트 입력들(803a, 803b, 803c, … 803n)로 분해한다. 넷(4)의 8-비트 입력들(803a, 803b, 803c, … 803n)은 이에 따라 비트들: b_0, b_1, b_2, … b_7; b_8, b_9, b_{10}, … b_{15}; b_{16}, b_{17}, b_{18}, … b_{23}; 및 b_{24}, b_{25}, b_{26}, … b_{31}로 표현될 수 있다. 각각의 NLTF 서브-회로(804, 806, 808, 810)는 그의 대응하는 입력을 수신하고 동일한 수의 비트(예를 들어, 8-비트) 출력들(805a, 805b, 805c, … 805n)을 생성할 수 있다. 연계 회로(812)는 이어서 32-비트 S-박스 A(814) 입력 값(y)을 생성하기 위해 이들 출력 값들(805a, 805b, 805c, … 805n)을 연계한다. 일 양상에 따라, 값들(m_1, m_2, m_3, 및 m_N)은 서로 동일하여서, 메인 입력(x)으로부터의 동일한 수의 비트가 각각의 NLTF 서브-회로(804, 806, 808, 810)에 송신된다. 다른 양상에 따라, 값들(m_1, m_2, m_3, 및 m_N)은 서로 동일한 것이 아니라, 값 n개의 비트들 미만이다.

[0051] [0050] 일 예에 따라, S-박스 A(814)는 도 3에서 도시된 S-박스(300)이다. 이에 따라, 도 3에서 도시된 프로세스와 유사하게, S-박스 A(814)는 중간 값을 생성하기 위해 입력 값(y) 및 32-비트 제 1 값에 대해 XOR 동작을 수행한다. 다음으로, S-박스 A(814)는 중간 값의 해밍 웨이트 만큼 중간 값을 (좌측 또는 우측으로) 회전시킨다. 결과적인 회전된 32-비트 값은 이어서 32-비트 메인 S-박스 출력 값(z)으로서 S-박스 A(814)로부터 출력된다. 32-비트 제 1 값은 (도 8에서 도시되지 않은) 회로에 의해 제공될 수 있고 (도 3에서 도시된 바와 같이) 상수 또는 (도 6 및 도 7에서 도시된 바와 같이) 가변적일 수 있다.

[0052]

[0053] **암호 값들을 생성하기 위한 예시적인 방법**

[0054] [0051] 도 9는 치환 박스(S-박스)와 연관되는 암호 값들을 생성하기 위한 방법의 흐름도(900)를 예시한다. 이 방법은 입력 값 및 제 1 값을 획득하는 것(902), 및 (A) 제 1 중간 값을 생성하기 위해 입력 값 및 제 1 값에 대해 비트와이즈 배타적 OR(XOR) 동작을 수행하는 것(906a), 및 S-박스 출력 값을 생성하기 위해 제 1 중간 값의 해밍 웨이트와 동일한 비트들의 수 만큼 제 1 중간 값에 대해 비트와이즈 회전 동작을 수행하는 것(908a), 또는 (B) 제 1 중간 값을 생성하기 위해 입력 값의 해밍 웨이트와 동일한 비트들의 수 만큼 입력 값에 대해 비트와이즈 회전 동작을 수행하는 것(906b), 및 S-박스 출력 값을 생성하기 위해 제 1 중간 값 및 제 1 값에 대해 비트와이즈 XOR 동작을 수행하는 것(908b), 또는 (C) 제 1 중간 값을 생성하기 위해 입력 값 및 제 1 값에 대해 비트와이즈 XOR 동작을 수행하는 것(906c), 제 2 중간 값을 생성하기 위해 제 1 중간 값의 해밍 웨이트와 동일한 비트들의 수 만큼 제 1 중간 값에 대해 비트와이즈 회전 동작을 수행하는 것(908c), 제 2 값을 획득하는 것(910c), 및 S-박스 출력 값을 생성하기 위해 제 2 중간 값 및 제 2 값에 대해 비트와이즈 XOR 동작을 수행하는 것(912c) 중 하나에 의해 S-박스 출력 값을 생성하는 것(904)을 포함한다.

[0055] **S-박스(들)를 포함하는 예시적인 전자 디바이스**

[0056] [0052] 도 10은 일 양상에 따라 본 명세서에서 설명되는 S-박스들(300, 400, 500, 800) 중 임의의 하나를 포함하는 전자 디바이스(1000)에 대한 하드웨어 구현의 개략적 블록도를 예시한다. 전자 디바이스(1000)는 모바일 전화, 스마트폰, 태블릿, 휴대용 컴퓨터, 및/또는 회로를 갖는 임의의 다른 전자 디바이스일 수 있다. 전자 디바이스(1000)는 통신 인터페이스(1010), 사용자 인터페이스(1012) 및 프로세싱 시스템(1014)을 포함할 수 있다. 프로세싱 시스템(1014)은 프로세싱 회로(예를 들어, 프로세서)(1004), 메모리 회로(예를 들어, 메모리)(1005), 컴퓨터-판독 가능한 저장 매체(1006), 버스 인터페이스(1008) 및 버스(1002)를 포함할 수 있다. 프로세싱 시스템(1014) 및/또는 프로세싱 회로(1004)는 도 3, 도 4, 도 5, 도 6, 도 7, 도 8, 및/또는 도 9에 관하여 위에서 설명된 S-박스들(300, 400, 500, 800) 및 다른 회로들 및/또는 모듈들(602, 702)에 관해 설명된 단계들, 기능들 및/또는 프로세스들 중 임의의 것을 수행하도록 구성될 수 있다.

[0057] [0053] 프로세싱 회로(1004)는 전자 디바이스(1000)에 대한 데이터를 프로세싱하도록 적응된 하나 또는 그 초과의 프로세서들(예를 들어, 제 1 프로세서 등)일 수 있다. 예를 들어, 프로세싱 회로(1004)는 도 9에서 설명된 단계들 중 임의의 하나를 수행하기 위한 수단으로서의 역할을 하는 주문형 집적회로(ASIC)와 같은 특수 프로세서일 수 있다. 즉, 프로세싱 회로(1004)는 입력 값 및 제 1 값을 획득하도록, 그리고 (A) 제 1 중간 값을 생성하기 위해 입력 값 및 제 1 값에 대해 비트와이즈 배타적 OR(XOR) 동작을 수행하는 것, 및 S-박스 출력 값을 생성하기 위해 제 1 중간 값의 해밍 웨이트와 동일한 비트들의 수 만큼 제 1 중간 값에 대해 비트와이즈 회전 동작을 수행하는 것, 또는 (B) 제 1 중간 값을 생성하기 위해 입력 값의 해밍 웨이트와 동일한 비트들의 수 만큼 입력 값에 대해 비트와이즈 회전 동작을 수행하는 것, 및 S-박스 출력 값을 생성하기 위해 제 1 중간 값 및 제 1 값에 대해 비트와이즈 XOR 동작을 수행하는 것, 또는 (C) 제 1 중간 값을 생성하기 위해 입력 값 및 제 1 값에 대해 비트와이즈 XOR 동작을 수행하는 것, 제 2 중간 값을 생성하기 위해 제 1 중간 값의 해밍 웨이트와 동일한 비트들의 수 만큼 제 1 중간 값에 대해 비트와이즈 회전 동작을 수행하는 것, 제 2 값을 획득하는 것, 및 S-박스 출력 값을 생성하기 위해 제 2 중간 값 및 제 2 값에 대해 비트와이즈 XOR 동작을 수행하는 것 중 하나에 의해, S-박스 출력 값을 생성하도록 구성될 수 있다.

[0058] [0054] 프로세싱 회로들(1004)의 예들은 마이크로프로세서, 마이크로제어기들, DSP들(digital signal processors), FPGA들(field programmable gate arrays), PLD들(programmable logic devices), 상태 머신들, 게이팅된 로직, 이산 하드웨어 회로들 및 본 개시를 통해 설명된 다양한 기능성을 수행하도록 구성된 다른 적합한 하드웨어를 포함한다. 프로세싱 회로(1004)는 또한 버스(1002)를 관리하고 컴퓨터-판독 가능한 저장 매체(1006) 및/또는 메모리(1005) 상에 저장된 소프트웨어를 실행하는 것을 담당한다. 소프트웨어는, 프로세싱 회로(1004)에 의해 실행될 때, 프로세싱 시스템(1014)으로 하여금 S-박스들(300, 400, 500, 800)에 관하여 위에서

설명된 다양한 기능들, 단계들 및/또는 프로세스들을 수행하게 한다. 컴퓨터-판독 가능한 저장 매체(1006)는 소프트웨어를 실행할 때, 프로세싱 회로(1004)에 의해 조작되는 데이터를 저장하기 위해 이용될 수 있다.

[0059] [0055] 메모리 회로(1005)는 플래시 메모리, 자기 또는 광학 하드 디스크 드라이브들 등과 같은(그러나 이들로 제한되지 않음) 비-휘발성 메모리일 수 있다. 몇몇 양상들에서, 섹터 정보 및/또는 오버헤드 메시지(구성 시퀀스 번호를 포함함)를 저장하는 메모리는 정보를 무기한으로 저장하도록 연속적으로 전력공급될 수 있는 DRAM(예를 들어, DDR, SDRAM), SRAM 등과 같은 휘발성 메모리일 수 있다.

[0060] [0056] 소프트웨어는, 소프트웨어, 펌웨어, 미들웨어, 마이크로코드, 하드웨어 기술 언어 또는 기타 등으로 지칭되든지 간에, 명령들, 명령 세트들, 코드, 코드 세그먼트들, 프로그램 코드, 프로그램들, 서브프로그램들, 소프트웨어 모듈들, 애플리케이션들, 소프트웨어 애플리케이션들, 소프트웨어 패키지들, 루틴들, 서브루틴들, 객체들, 실행 가능한 것들, 실행 스레드들, 프로시저들, 함수들 등을 의미하도록 광의로 해석되어야 한다. 소프트웨어는 컴퓨터-판독 가능한 저장 매체(1006) 상에 상주할 수 있다. 컴퓨터-판독 가능한 저장 매체(1006)는 비-일시적인 컴퓨터-판독 가능한 저장 매체일 수 있다. 비-일시적인 컴퓨터-판독 가능한 저장 매체는 예로서, 자기 저장 디바이스(예를 들어, 하드디스크, 플로피디스크, 자기 스트립), 광학 디스크(예를 들어, 컴팩트 디스크(CD) 또는 디지털 다용도 디스크(DVD), 스마트 카드, 플래시 메모리 디바이스(예를 들어, 카드, 스틱 또는 키 드라이브), RAM(random access memory), ROM(read only memory), PROM(programmable ROM), EPROM(erasable PROM), EEPROM(electrically erasable PROM), 레지스터, 제거 가능한 디스크, 및 컴퓨터에 의해 액세스되고 판독될 수 있는 소프트웨어 및/또는 명령들을 저장하기 위한 임의의 다른 적합한 매체를 포함한다. 컴퓨터-판독 가능한 저장 매체는 예로서, 반송파, 전송 라인 및 컴퓨터에 의해 액세스되고 판독될 수 있는 소프트웨어 및/또는 명령들을 전송하기 위한 임의의 다른 적합한 매체를 또한 포함할 수 있다. 컴퓨터-판독 가능한 저장 매체(1006)는 프로세싱 시스템(1014) 내에, 프로세싱 시스템(1014) 외부에, 또는 프로세싱 시스템(1014)을 포함하는 다수의 엔티티에 걸쳐서 분산된 채로 상주할 수 있다. 컴퓨터-판독 가능한 저장 매체(1006)는 컴퓨터 프로그램 물건에서 실현될 수 있다.

[0061] [0057] 이 예에서, 프로세싱 시스템(1014)은 버스(1002)에 의해 일반적으로 표현되는 버스 아키텍처를 갖도록 구현될 수 있다. 버스(1002)는 전체 설계 제약들 및 프로세싱 시스템(1014)의 특정한 애플리케이션에 의존하여 임의의 수의 상호연결 버스들 및 브리지들을 포함할 수 있다. 버스(1002)는 (일반적으로 프로세서(1004)에 의해 표현되는) 하나 또는 그 초과의 프로세서들, 메모리(1005) 및 (일반적으로 컴퓨터-판독 가능한 저장 매체(1006)에 의해 표현되는) 컴퓨터-판독 가능한 매체들을 포함하는 다양한 회로들을 함께 링크한다. 버스(1002)는 또한 당 분야에 잘 알려진 타이밍 소스들, 주변장치들, 전압 레귤레이터들 및 전력 관리 회로들과 같은 다양한 다른 회로들을 링크할 수 있으며, 이에 따라 더 이상 추가로 설명되지 않을 것이다. 버스 인터페이스(1008)는 (만약 있다면) 버스(1002)와 통신 인터페이스(1010) 간의 인터페이스를 제공한다. 통신 인터페이스(1010)는 전송 매체 상에서 다른 장치와 통신하기 위한 수단을 제공한다. 장치의 성질에 의존하여, 사용자 인터페이스(1012)(예를 들어, 키패드, 디스플레이, 스피커, 마이크로폰, 터치스크린 디스플레이 등)는 또한 전자 디바이스(1000)에 제공될 수 있다.

[0062] [0058] 도 11은 본 개시의 일 양상에 따른 프로세서(1004)의 개략적 블록도를 예시한다. 프로세서(1004)는 다른 것들 중에서, 메인 입력 값, 입력 값, 제 1 값 및/또는 제 2 값 획득 회로(1102)를 포함한다. 획득 회로(1102)는 메인 입력 값, 입력 값, 제 1 값 및/또는 제 2 값을 획득하기 위한 수단의 일 예로서의 역할을 한다. 프로세서(1004)는 추가로 도 8에 관하여 위에서 설명된 바와 같이 NLTF를 실행하도록 구성되는 비-선형 변환 함수 회로(1104)를 포함한다.

[0063] [0059] 도 3, 도 4, 도 5, 도 6, 도 7, 도 8, 도 9, 도 10, 및/또는 도 11에서 예시된 컴포넌트들, 단계들, 특징들 및/또는 기능들 중 하나 이상은 단일의 컴포넌트, 단계, 특징 또는 함수로 재배열되고 그리고/또는 결합될 수 있거나, 또는 몇 개의 컴포넌트들, 단계들 또는 함수들에서 실현될 수 있다. 부가적인 엘리먼트들, 컴포넌트들, 단계들 및/또는 함수들은 본 발명으로부터 벗어남 없이 또한 부가될 수 있다. 도 3, 도 4, 도 5, 도 6, 도 7, 도 8, 도 9, 도 10, 및/또는 도 11에서 예시된 장치들, 디바이스들 및/또는 컴포넌트들은 도 9에서 설명된 방법들, 특징들, 또는 단계들 중 하나 이상을 수행하도록 구성될 수 있다. 본 명세서에서 설명된 알고리즘들은 또한 효과적으로 소프트웨어로 구현되고 그리고/또는 하드웨어에 임베딩될 수 있다.

[0064] [0060] 또한, 본 개시의 일 양상에서, 도 10 및/또는 도 11에서 예시되는 프로세싱 회로(1004)는 도 9에서 설명된 알고리즘들, 방법들 및/또는 단계들을 수행하도록 특별히 설계되고 그리고/또는 하드-와이어링되는 특수 프로세서(예를 들어, 주문형 집적 회로(예를 들어, ASIC))일 수 있다. 따라서, 이러한 특수 프로세서(예를 들어,

ASIC)는 도 9에서 설명된 알고리즘들, 방법들 및/또는 단계들을 실행하기 위한 수단의 일 예일 수 있다. 컴퓨터-판독 가능한 저장 매체(1006)는 특수 프로세서(예를 들어, ASIC)에 의해 실행될 때, 특수 프로세서로 하여금 도 9에서 설명된 알고리즘들, 방법들 및/또는 단계들을 수행하게 하는 프로세서(1004) 판독 가능한 명령들을 또한 저장할 수 있다.

[0065] [0061] 또한, 본 개시의 양상들은 흐름 차트, 흐름도, 구조도, 또는 블록도로서 도시된 프로세스로서 설명될 수 있다는 것에 주의한다. 흐름 차트가 순차적인 프로세스로서 동작들을 설명할 수 있지만, 동작들 대부분은 병렬로 또는 동시에 수행될 수 있다. 또한, 동작들의 순서는 재배열될 수 있다. 프로세스는 그의 동작들이 완료될 때 종결된다. 프로세스는 방법, 함수, 프로시저, 서브루틴, 서브프로그램 등에 대응할 수 있다. 프로세스가 함수에 대응할 때, 그의 종결은 메인 함수 또는 호출 함수로의 함수의 복귀에 대응할 수 있다.

[0066] [0062] 또한, 저장 매체는 정보를 저장하기 위한 ROM(read-only memory), RAM(random access memory), 자기 디스크 저장 매체들, 광학 저장 매체들, 플래시 메모리 디바이스들 및/또는 다른 기계-판독 가능한 매체들 및 프로세서-판독 가능한 매체들 및/또는 컴퓨터-판독 가능한 매체들을 비롯해서, 데이터를 저장하기 위한 하나 또는 그 초과의 디바이스들을 나타낼 수 있다. "기계-판독 가능한 매체", "컴퓨터-판독 가능한 매체" 및/또는 "프로세서-판독 가능한 매체"란 용어들은 휴대식 또는 고정식 저장 디바이스들, 광학 저장 디바이스들 및 명령(들) 및/또는 데이터를 저장, 포함 또는 전달할 수 있는 다양한 다른 매체들과 같은 비-일시적인 매체들을 포함(그러나 이들로 제한되지 않음)할 수 있다. 따라서, 본 명세서에서 설명된 다양한 방법들은 완전히 또는 부분적으로, "기계-판독 가능한 매체", "컴퓨터-판독 가능한 매체", 및/또는 "프로세서-판독 가능한 매체"에 저장되고 하나 또는 그 초과의 프로세서들, 기계들 및/또는 디바이스들에 의해 실행되는 명령들 및/또는 데이터에 의해 구현될 수 있다.

[0067] [0063] 또한, 본 개시의 양상들은 하드웨어, 소프트웨어, 펌웨어, 미들웨어, 마이크로코드 또는 이들의 임의의 결합에 의해 구현될 수 있다. 소프트웨어, 펌웨어, 미들웨어 또는 마이크로코드에서 구현될 때, 필요한 작업들을 수행하기 위한 프로그램 코드 또는 코드 세그먼트들은 저장 매체 또는 다른 저장소(들)와 같은 기계-판독 가능한 매체에 저장될 수 있다. 프로세서는 필수 작업들을 수행할 수 있다. 코드 세그먼트는 프로시저, 함수, 서브프로그램, 프로그램, 루틴, 서브루틴, 모듈, 소프트웨어 패키지, 클래스 또는 명령들, 데이터 구조들, 또는 프로그램 스테이트먼트들의 임의의 결합을 나타낼 수 있다. 코드 세그먼트는 정보, 데이터, 인수들, 파라미터들 또는 메모리 콘텐츠들을 전달 및/또는 수신함으로써 다른 코드 세그먼트 또는 하드웨어 회로에 커플링될 수 있다. 정보, 인수들, 파라미터들, 데이터 등은 메모리 공유, 메시지 전달, 토큰 전달, 네트워크 전송 등을 포함하는 임의의 적합한 수단을 통해 전달, 포워딩 또는 전송될 수 있다.

[0068] [0064] 본 명세서에서 개시된 예들과 관련하여 설명되는 다양한 예시적인 논리적 블록들, 모듈들, 회로들 엘리먼트들 및/또는 컴포넌트들은 범용 프로세서, DSP(digital signal processor), ASIC(application specific integrated circuit), FPGA(field programmable gate array), 또는 다른 프로그래밍 가능한 로직 컴포넌트, 이산 게이트 또는 트랜지스터 로직, 이산 하드웨어 컴포넌트들, 또는 본 명세서에서 설명된 기능들을 수행하도록 설계된 이들의 임의의 결합으로 구현되거나 수행될 수 있다. 범용 프로세서는 마이크로프로세서일 수 있지만, 대안적으로, 프로세서는 임의의 종래의 프로세서, 제어기, 마이크로제어기, 또는 상태 머신일 수 있다. 프로세서는 또한, 컴퓨팅 컴포넌트들의 결합, 예를 들어, DSP 및 마이크로프로세서의 결합, 다수의 마이크로프로세서들, DSP 코어에 결합되는 하나 또는 그 초과의 마이크로프로세서들, 또는 임의의 다른 이러한 구성으로서 구현될 수 있다.

[0069] [0065] 본 명세서에서 개시된 예들과 관련하여 설명되는 방법들 또는 알고리즘들은 프로세싱 유닛, 프로그래밍 명령들, 또는 다른 지시들의 형태로, 직접 하드웨어로, 프로세서에 의해 실행 가능한 소프트웨어 모듈로, 또는 이들 둘의 결합으로 실현될 수 있고, 다수의 디바이스에 걸쳐 분산되거나 단일 디바이스에 포함될 수 있다. 소프트웨어 모듈은 RAM 메모리, 플래시 메모리, ROM 메모리, EPROM 메모리, EEPROM 메모리, 레지스터들, 하드디스크, 제거 가능한 디스크, CD-ROM, 또는 당 분야에 알려진 임의의 다른 형태의 저장 매체에 상주할 수 있다. 저장 매체는 프로세서에 커플링될 수 있어서, 프로세서는 저장 매체로부터 정보를 판독하고 저장 매체에 정보를 기록할 수 있게 된다. 대안적으로, 저장 매체는 프로세서에 통합될 수 있다.

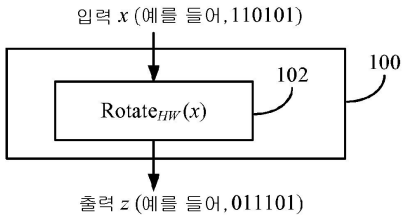
[0070] [0066] 당업자들은 추가로, 본 명세서에서 개시된 양상들과 관련하여 설명된 다양한 예시적인 논리적 블록들, 모듈들, 회로들 및 알고리즘 단계들이 전자 하드웨어, 컴퓨터 소프트웨어, 또는 이들 둘의 결합들로서 구현될 수 있다는 것을 인지할 것이다. 하드웨어 및 소프트웨어의 이러한 상호교환성을 명확하게 예시하기 위해, 다양한 예시적인 컴포넌트들, 블록들, 모듈들, 회로들 및 단계들은 그들의 기능성의 견지에서 일반적으로 위에서 설

명되었다. 이러한 기능성이 하드웨어 또는 소프트웨어로서 구현될지 여부는 전체 시스템에 부과되는 설계 제약들 및 특정한 애플리케이션에 의존한다.

[0071] [0067] 본 명세서에서 설명된 발명의 다양한 특징들은 본 발명으로부터 벗어남 없이 상이한 시스템들에서 구현될 수 있다. 본 개시의 위의 양상들은 단지 예들일 뿐이며 본 개시를 제한하는 것으로서 의도되지 않는다는 것에 주의되어야 한다. 본 개시의 양상들의 설명은 청구항의 범위를 제한하는 것이 아니라 예시하는 것으로 의도된다. 이에 따라, 본 개시는 다른 타입들의 장치들에 쉽게 적용될 수 있고, 다수의 대안들, 변형들 및 변동물들이 당업자들에게 자명하게 될 것이다.

도면

도면1



(종래기술)

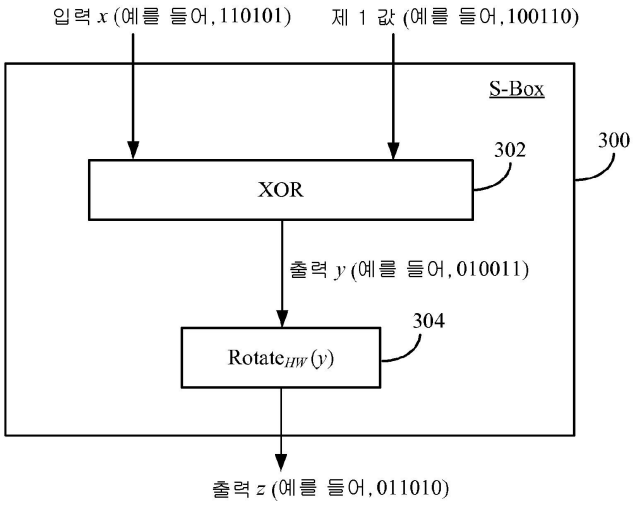
도면2

출력 z 비트	값	HWBF
LSB	1	$W(x)$
2nd LSB	0	$W(x<<1)$
3rd LSB	1	$W(x<<2)$
4th LSB	1	$W(x<<3)$
5th LSB	1	$W(x<<4)$
6th LSB	0	$W(x<<5)$

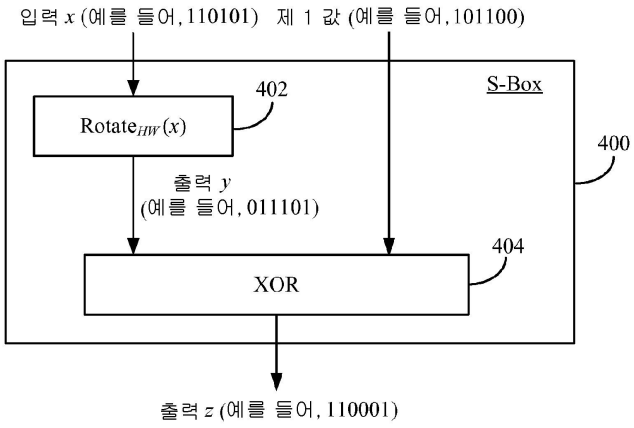
200

(종래기술)

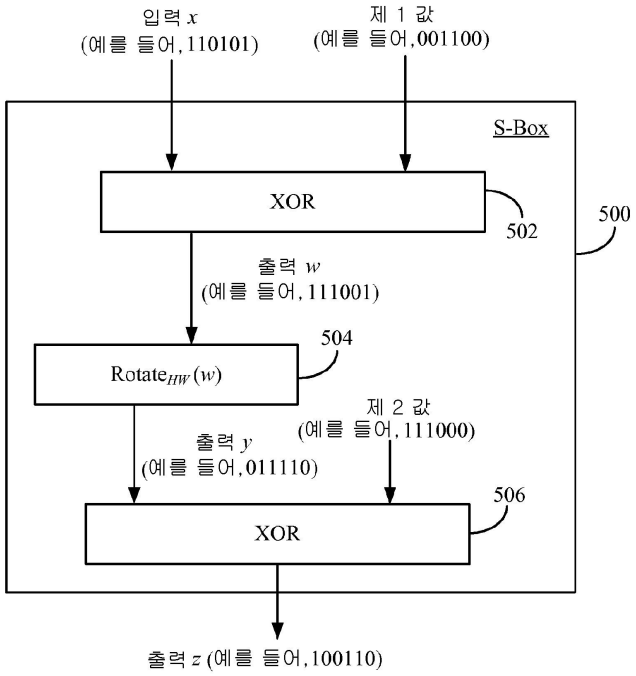
도면3


입력 x (예를 들어, 110101)
제 1 값 (예를 들어, 100110)
S-Box
300
302
XOR
출력 y (예를 들어, 010011)
304
Rotate$_{HW}$(y)
출력 z (예를 들어, 011010)

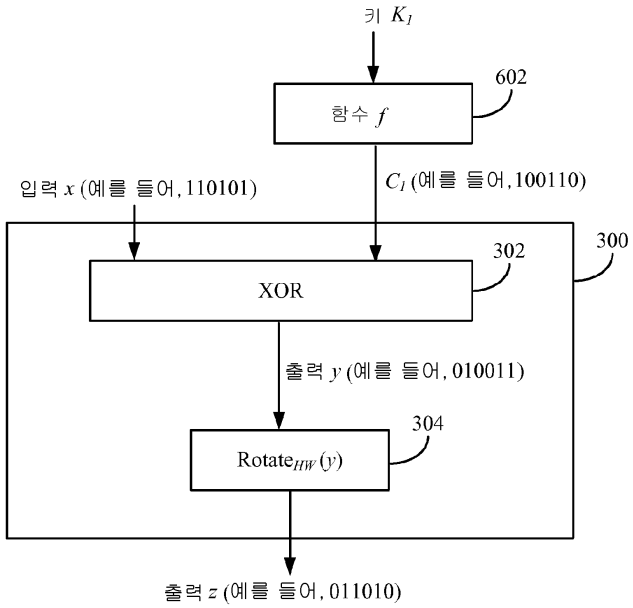
도면4


입력 x (예를 들어, 110101)
제 1 값 (예를 들어, 101100)
S-Box
402
Rotate$_{HW}$(x)
400
출력 y
(예를 들어, 011101)
404
XOR
출력 z (예를 들어, 110001)

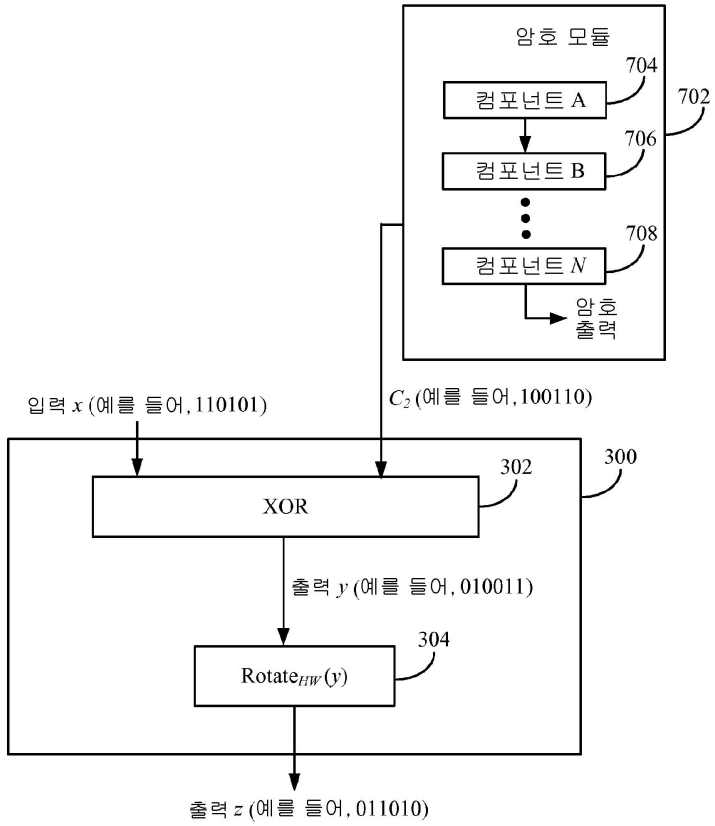
도면5


입력 x
(예를 들어, 110101)
제 1 값
(예를 들어, 001100)
S-Box
XOR
502
500
출력 w
(예를 들어, 111001)
504
Rotate$_{HW}$(w)
제 2 값
(예를 들어, 111000)
출력 y
(예를 들어, 011110)
506
XOR
출력 z (예를 들어, 100110)

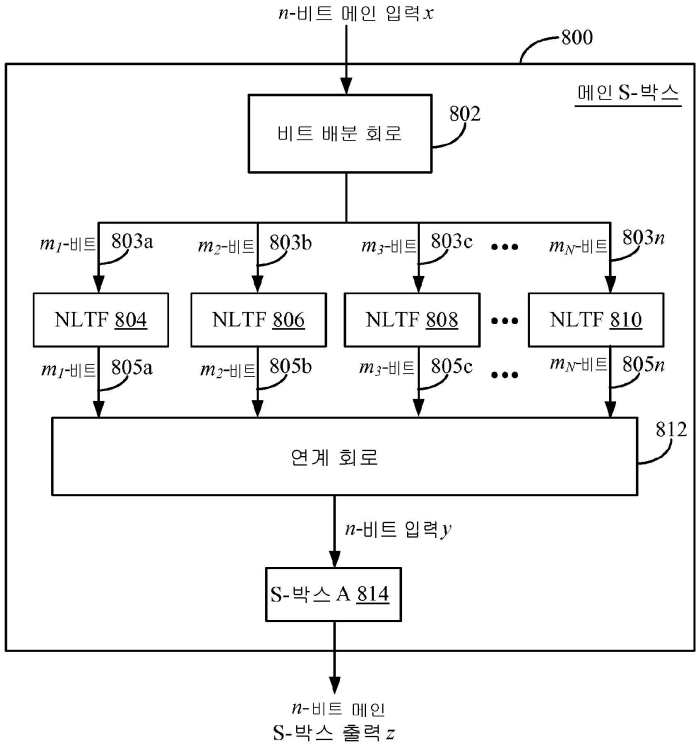
도면6


키 K_1
602
함수 f
C_1 (예를 들어, 100110)
입력 x (예를 들어, 110101)
300
302
XOR
출력 y (예를 들어, 010011)
304
Rotate$_{HW}$(y)
출력 z (예를 들어, 011010)

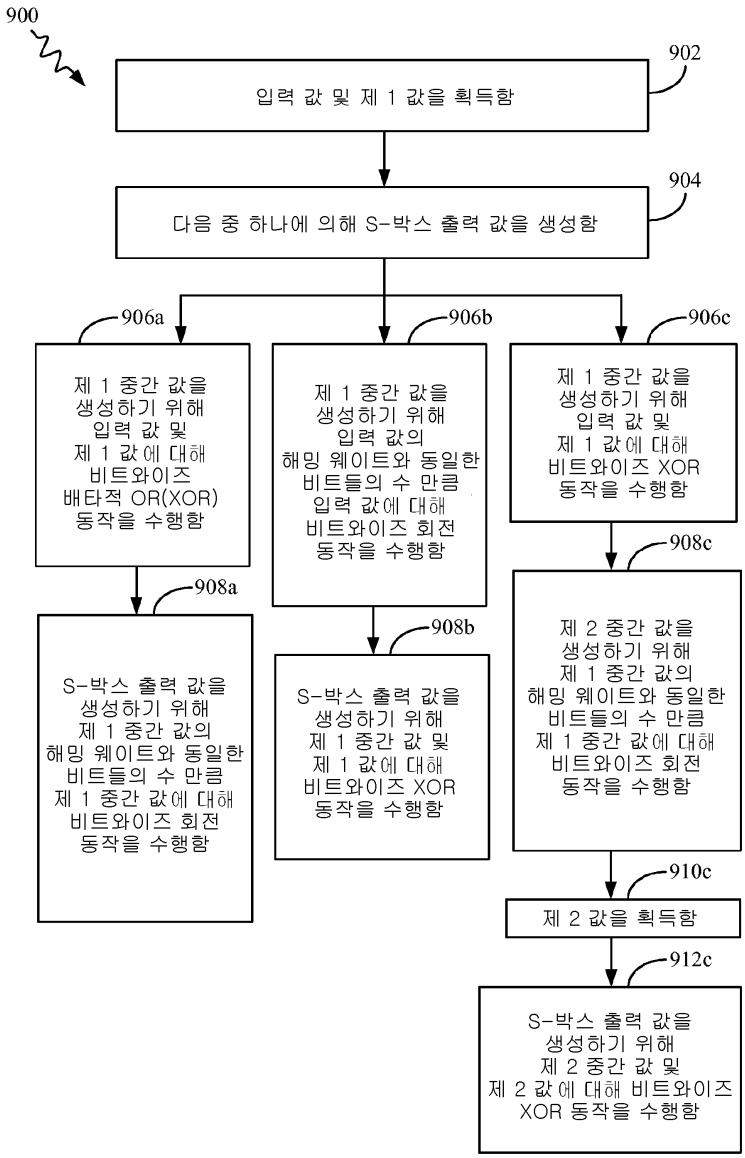
도면7


암호 모듈
704
컴포넌트 A
702
706
컴포넌트 B
708
컴포넌트 N
암호 출력
입력 x (예를 들어, 110101)
C2 (예를 들어, 100110)
300
302
XOR
출력 y (예를 들어, 010011)
304
RotateHW(y)
출력 z (예를 들어, 011010)

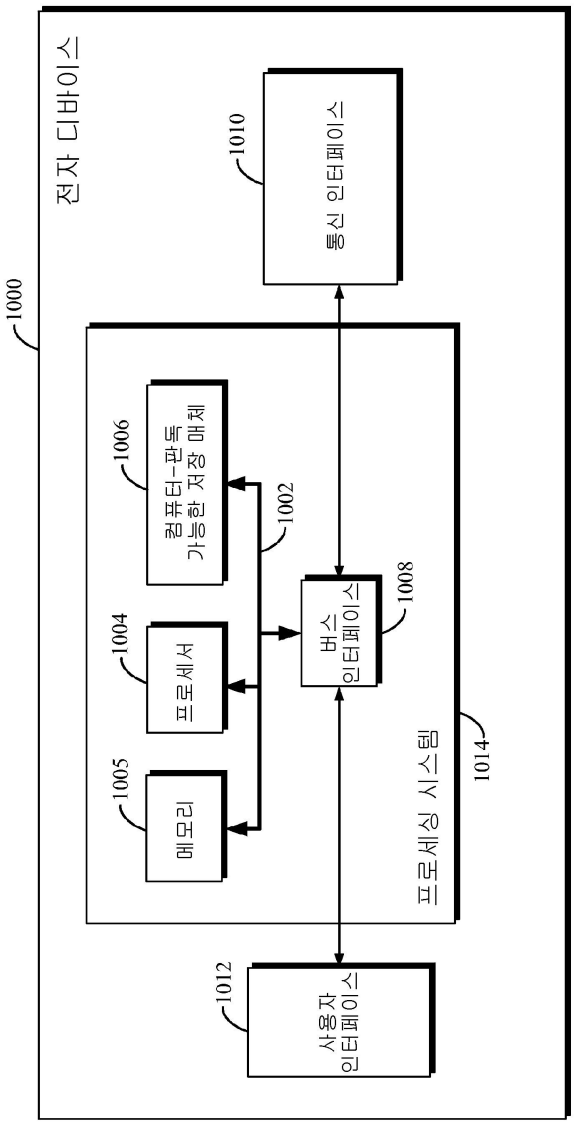
도면8


n-비트 메인 입력 x
800
메인 S-박스
비트 배분 회로
802
m1-비트
803a
m2-비트
803b
m3-비트
803c
mN-비트
803n
NLTF 804
NLTF 806
NLTF 808
NLTF 810
m1-비트
805a
m2-비트
805b
m3-비트
805c
mN-비트
805n
812
연계 회로
n-비트 입력 y
S-박스 A 814
n-비트 메인
S-박스 출력 z

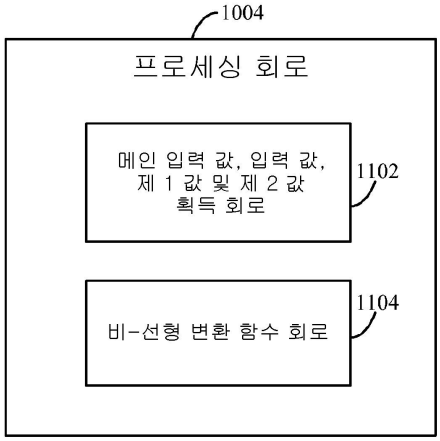
도면9


900
902
입력 값 및 제 1 값을 획득함
904
다음 중 하나에 의해 S-박스 출력 값을 생성함
906a
제 1 중간 값을 생성하기 위해 입력 값 및 제 1 값에 대해 비트와이즈 배타적 OR(XOR) 동작을 수행함
906b
제 1 중간 값을 생성하기 위해 입력 값의 해밍 웨이트와 동일한 비트들의 수 만큼 입력 값에 대해 비트와이즈 회전 동작을 수행함
906c
제 1 중간 값을 생성하기 위해 입력 값 및 제 1 값에 대해 비트와이즈 XOR 동작을 수행함
908a
S-박스 출력 값을 생성하기 위해 제 1 중간 값의 해밍 웨이트와 동일한 비트들의 수 만큼 제 1 중간 값에 대해 비트와이즈 회전 동작을 수행함
908b
S-박스 출력 값을 생성하기 위해 제 1 중간 값 및 제 1 값에 대해 비트와이즈 XOR 동작을 수행함
908c
제 2 중간 값을 생성하기 위해 제 1 중간 값의 해밍 웨이트와 동일한 비트들의 수 만큼 제 1 중간 값에 대해 비트와이즈 회전 동작을 수행함
910c
제 2 값을 획득함
912c
S-박스 출력 값을 생성하기 위해 제 2 중간 값 및 제 2 값에 대해 비트와이즈 XOR 동작을 수행함

도면10


전자 디바이스
1000
통신 인터페이스
1010
컴퓨터-판독 가능한 저장 매체
1006
1002
버스 인터페이스
1008
프로세서
1004
메모리
1005
프로세싱 시스템
1014
사용자 인터페이스
1012

도면11


1004
프로세싱 회로
메인 입력 값, 입력 값, 제 1 값 및 제 2 값 획득 회로
1102
비-선형 변환 함수 회로
1104