(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl. [6]
H04N 7/16

(45) 공고일자 2002년06월26일
(11) 등록번호 10-0324859
(24) 등록일자 2002년02월04일

(21) 출원번호 10-1994-0028886
(22) 출원일자 1994년11월04일

(65) 공개번호 특1995-0023025
(43) 공개일자 1995년07월28일

(30) 우선권주장 08/167,781 1993년12월21일 미국(US)

(73) 특허권자 제너럴 인스트루먼트 코포레이션
매클린토크 샤운 엘
미합중국 19044 펜실베니아주 호샴 투어나먼트 드라이브 101

(72) 발명자 에릭스프링크
미합중국,92009캘리포니아,칼스베드,코트다이아나2948

(74) 대리인 김윤배
이범일

심사관 : 변형철

(54) 암호화알고리즘의상보성을피하기위한장치

요약

본 발명은, 종래의 수행에 의해 제공된 상보성의 약점을 극복하는 DES처럼 보안성 알고리즘의 수행이 제공된다. DES 실행에서, 암호화 프로세서는 데이터 블록에 DES를 공급한다. DES프로세서는 데이터 블록을 수신하기 위한 제1입력 포트와, 암호화 키를 수신하기 위한 제2입력 포트 및, 암호화 후 데이터 블록을 출력하기 위한 출력 포트를 포함한다. 상보성을 갖지 않는 비선형 함수는 적어도 하나의 포트에 공급된다. 비선형 함수는 DES S-Box로부터 유리하게 도출될 수 있는 조사 테이블을 구성할 수 있다.

대표도

도 1

명세서

도면의 간단한 설명

제1도는 종래 암호화 알고리즘의 수행을 도시하는 블록도,

제2도는 본 발명에 따른 암호화 알고리즘을 수행하는 장치의 블록도이다.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

[산업상의 이용분야]

본 발명은, 일반적으로 정보처리 시스템용 보안장치에 관한 것으로, 특히 상보특성이 없는 암호화 알고리즘을 수행하기 위한 장치에 관한 것이다.

본 발명은 비록 그것이 그런 사용에 결코 제한되지 않더라도 스크램블된 텔레비젼 신호의 정확한 전송에 특히 적용할 수 있다.

[종래의 기술 및 문제점]

텔레비젼 신호의 원격 디스크램블링을 제어하기 위한 많은 구성이 있는 바, 이러한 구성은 위성 텔레비젼 시스템과 케이블 텔레비젼 시스템을 포함하는 가입자 텔레비젼 시스템에서 보안성을 유지하기 위해 필요하다. 대표적으로, 시스템 가입자는 텔레비젼 신호원(예컨대, 케이블 장치 또는 위성 수신장치)과 텔레비젼 세트 사이에 연결된 디스크램블러를 갖추고 있다. 각 가입자의 디스크램블러는 특별한 유료 스포츠 경기 또는 홈 박스 오피스(Home Box Office) 영화채널처럼 특별한 서비스를 수령할 수 있거나 또는 수령할 수 없도록 시스템 운영자에 의해 원격적으로 억세스된다. 이런 시스템의 한가지 문제는 " 해적들" 이 시스템의 보안성을 해치는 경향이 있고, 받은 서비스에 대한 돈의 지불없이 모든 프로그래밍의 수령이 가능한 " 블랙박스" 를 파는 것이다. 해적문제로 싸우는 것은 시스템 동작자에 대해 비싸고, 어려웠다. 특별한 보안성 시스템이 깨지는 것과 동시에, 시스템 동작자는 일반적으로 다른 보안성 알고리즘으로 동작하는 새로운 단위로 모든 존재하는 디스크램블러를 바꿔야 한다. 이런 해결은 비용면에서 효과적이지 않다.

여러가지 시스템은 해적행위를 하기에 더 어렵도록 디자인되었다. 그런 시스템의 하나는 길하우슨과 기타에 의해 미국 특허 제4,613,901호에 " 텔레비젼 신호의 선택적 원거리 디스크램블링과 제어 스크램블링을 위한 분포 시스템 및 신호 암호화" 라는 제목으로 공개되었다. 길하우슨과 기타 시스템에서, " 작업키" 신호는 알고리즘이 공통 카테고리 키 신호 또는 다소 다른 키신호에 의해 암호화화된 후, 잘 알려진 DES 보안성 알고리즘에 따라 발생된다. 유일한 암호화 키 스트림은 알고리즘이 작업 키 신호에 의해 맞추어질 때 DES 알고리즘에 따른 초기 벡터신호를 처리하는 것에 의해 발생된다. 텔레비젼 신호는 스크램블된 텔레비젼 신호를 공급하기 위한 유일한 암호화 키 스트림에 따라 스크램블된다. 다른 선택된 가입자의 디스크램블러에 개별적으로 어드레스된 다수의 유일한 암호화된 카테고리 키 신호는 알고리즘이 다른 디스크램블러와 관련된 다수의 다른 " 단위 키" 신호에 의해 암호화화될 때 DES알고리즘에 따라 초기의 공통 카테고리 키 신호를 처리하는 것에 의해 발생된다. 스크램블된 텔레비젼 신호와, 초기화 벡터 신호 및, 다수의 암호화된 카테고리 키 신호는 디스크램블러들에게 방송된다. 각 디스크램블러에서 암호 키 스트림은 텔레비젼 신호를 디스크램블하기 위해 재생된다. 각 디스크램블러는 디스크램블러가 유일한 암호화된 카테고리 키 신호에 의해 어드레스될 때 공통 카테고리 키 신호를 재생하는데 이용하기 위해 메모리에 저장된 유일한 단위 키 신호를 갖는다. DES 알고리즘을 사용하는 것에 의해, 길하우스 기타 시스템은 작업키를 재생함에 있어 해적에 대해 어렵고, 비싸게 만드는 높은 수준의 보안성을 제공한다.

길하우스 등처럼 보안성 시스템에 의한 DES 알고리즘에 대한 신뢰는 깨졌던적이 있는 DES 보안성을 공격하기 위한 약점이 있는 시스템이 되게 한다. 비록 아무도 데이터에 DES 알고리즘을 공적으로 파괴하지 않는다해도 약점은 보호되지 않았다. 약점은 DES 알고리즘처럼 암호 알고리즘의 " 보안특성" 으로부터 생긴다. 비록 이 약점이 알고리즘이 깨지는 것을 허락하지 않는다 해도, 부가적인 보안성은 보안특성이 제거된다면 길하우스 등에 의해 공개된 키 권력자에 특히 제공될 것이다.

보안특성의 결과로, 만약 프로세서에 확실한 데이터와 키 입력이 둘다 반전된다면 이 암호 프로세서의 출력은 반전될 것이다. 이것은 다음과 같이 수학적으로 설명될 수 있다.

$$E_K[X] = Y \rightarrow E_{\overline{K}}[\overline{X}] = \overline{Y}$$

여기서, X는 암호화 되는 데이터;

K는 안전한 암호화 키;

Y는 암호화된 데이터.

이러한 상보성은 원격적으로 선형인 DES의 단지 알려진 특성이다. 이러한 기술에서 알고리즘에 의해 제공된 보안성을 구성하기 위한 전위를 갖춘 DES와 같은 보안성 알고리즘에서 선형특성의 존재를 인정하게 된다.

DES 알고리즘에 관한 상세한 논의는 FIPS Pub. 74와, 1981년 4월 1일 " NBS 데이터 암호화 표준을 사용하고 효과를 주기 위한 안내" 및, 1977년 1월 15일 " 데이터 암호화 표준을 발표함" , 미국 상공부, 국제 표준국에 의해 논쟁이 된 연방 정보처리 표준 발표 46(" FIPS Pub, 46")에서 알려졌다. FIPS Pub. 74의 제3.6과 4절 5-7중의 " DES 알고리즘의 특성" 은 암암리에 상보특성을 상기시킨다. 또한, 특성은 데이비스, 도날드W의 " 방송망에서 데이터의 보안성(IEE 카달로그 제 EH0183-4호, 1981, p. 7.)" 에서 주장되었다.

상보성 없는 암호화 알고리즘을 수행하기 위한 장치를 제공하는데 유용하고, 이러한 암호화 알고리즘은 다른 암호화나 상보성을 갖는 해싱 함수뿐만 아니라 DES를 포함게 된다.

[발명의 목적]

본 발명은 상기한 점을 감안하여 발명된 것으로, 데이터 암호화 표준 또는 상보특성을 갖춘 소정의 암호화나 해싱 알고리즘을 이용해서 안전한 데이터 통신용으로 제공되는 장치를 제공함에 그 목적이 있다.

[발명의 구성 및 작용]

상기 목적을 달성하기 위한 본 발명은, 암호화 수단은 데이터 블록에 알고리즘을 공급한다. 암호화 수단은 데이터 블록을 수신하기 위한 제1입력 포트와, 암호화 키를 수신하기 위한 제2입력 포트 및, 상기 키를 기초로 한 알고리즘에 의해 처리된 후 데이터 블록을 출력하기 위한 출력 포트를 포함한다. 수단은 암호법 수단의 외면상, 상보성을 갖지 않는 함수를 공급하기 위한 적어도 하나의 포트에 조합된다. 또한, 이 함수는 비선형일 수 있다.

상기 함수를 공급하기 위한 수단은 조사 테이블을 구성할 수 있다. 조사 테이블은 DES 치환 상자(" S-Box")로부터 도출될 수 있다.

상기 함수를 공급하기 위한 수단은 제1입력 포트와, 제2입력 포트, 출력 포트 및, 그의 어떤 조합에 결합될 수 있다. 더욱이, 함수가 포트들중 하나 이상 공급된 곳에서, 이들 포트는 그곳에 공급된 같은 함수 또는 다른 함수를 가질 수 있다.

본 발명의 장치는 데이터 스트림을 해석하기 위한 수신기와 데이터 흐름을 암호화하기 위한 송신기 양쪽에서 제공된다. 암호화 수단의 외면상상보성 없는 함수를 공급하는 것에 의해 적용된 암호화나 해싱 알고리즘(예컨대, DES)의 암호화의 암호화 강도는 어떤 방법으로도 감소되지 않는다.

(실시예)

본 발명은 상보특성을 갖는 해싱 함수 또는 소정의 암호화 알고리즘의 잠정적 약점을 극복한다. 상보성은 DES 알고리즘의 단지 원격적인 선형특성과 예컨대, 입력 데이터 스트림과 키가 반전된다면 출력의 반전의 결과로 증명된다.

제1도는 DES 알고리즘과 같은 암호화 알고리즘의 종래의 기술의 수행을 도시한 것으로, 알고리즘은 잘 알려진 암호화 프로세서(10)에 의해 제공된다. 암호화 프로세서는 터미널(14)을 매개로 암호화되는 데이터 " X" 의 블록을 수신하고, 암호화 키 " K" 는 터미널(12)을 매개로 입력된다. 키 K에 의해 암호화된 데이터 블록 X는 암호화된 신호 Y와 같이 라인(16)을 매개로 암호화 프로세서(10)로부터 출력된다. 다음 설명에서, 암호화 프로세서(10)는 DES 프로세서이고, 비록 상보성을 가지는 어떤 다른 암호화 알고리즘이 치환될 수 있다 할지라도 그것의 보안성은 본 발명에 따라 향상된다.

제1도의 DES 수행에 의해 제공되는 암호화처리는 수학적으로 다음과 같이 표현될 수 있다.:

$$Y = X \oplus E_K[X]$$

DES알고리즘의 상보성에 기인하여 역수 또한 그런 참값을 유지한다:

$$\overline{Y} = \overline{X} \oplus E_{\overline{K}}[\overline{X}]$$

통신 보안성을 처리할 수 있는 상보특성을 극복하기 위해, 본 발명은 DES 프로세서의 외면상 상보성 갖지 않는 기능을 적용한다. 상보성 없는 비선형 함수가 각각 데이터 스트림과, 암호화 키 및, 암호화 프로세서로부터 출력에 공급되는 것에서 실시된 수행이 제2도에 도시되어 있다. 제1비선형 함수(f_1)는 조사 테이블 또는 디지탈 회로(20)에 의해 데이터 스트림에 공급된다. 제2비선형 함수(f_2)는 조사 테이블 또는 회로(22)를 매개로 암호화 키 K에 적용된다. 결과적인 데이터 스트림(X')과 암호화 키(K')는 라인(15)을 매개로 출력을 위한 데이터 스트림(X')을 암호화하기 위한 프로세서(10)에 의해 처리된다. 제3비선형 함수(f_3)는 조사 테이블 또는 디지탈 회로(24)를 매개로 암호화된 출력에 공급된다. 결과가 라인(16)상의 최종 출력(Y')이다. 본 발명을 수행하기 위해 제1도의 암호화 프로세서(10)는 제2도의 회로(10')로 간단히 대체될 수 있음에 주목한다.

비록, 제2도가 디지탈 회로(20,22,24) 또는 조사 테이블에 의해 비선형 함수의 적용을 묘사한다해도, 묘사된 3개의 모든 조사 테이블 또는 회로를 공급하는 것은 필요치 않다. 실제로, 상보성을 갖지 않는 단지 하나의 함수가 제2도에서 도시된 3개 위치의 어딘가에 공급될 수 있다. 묘사된 것처럼 함수가 하나의 위치 이상에 공급되는 곳에서, 상보성 없는 같은 함수는 각각 위치에 공급될 수 있거나 또는 상보성 없는 다른 함수는 각각 다른 위치에서 사용될 수 있다. 즉, f_1와, f_2 및, f_3은 모두 같은 함수에 있을 수 있거나 또는 모두 다른 함수 또는 그의 어떤 조합에 있을 수 있었다.

본 발명에 따라 사용되는 함수는 여러가지 방법으로 공급될 수 있다. 상기한 바와 같이, 함수는 상보특성을 유지하지 않기 위한 함수를 산출하는 조사 테이블 또는 적당한 논리를 구성할 수 있다. 실시예에서, 단순한 역이 아닌 조사 테이블이 사용된다. 원하는 결과를 제공하기 위해, 함수는 XOR동작을 거쳐 틀림없이 역이 아닌 테이블에 의해 수행된다. 또한, 표는 일대일 대응이어야 하고, 그런 것은 각 입력을 위해 하나의 출력을 갖는다. 일대일 대응인 테이블을 제공하는

것에 의해, 그것은 전환 테이블을 거쳐 역으로 될 것이다(예컨대, 디코더에서).

이러한 조사 테이블를 위해 많은 선택이 있다. 최소한의 요구는 일대일 대응 2비트 조사 테이블의 24버전중 하나를 공급하는 것이다. 이 24쌍으로부터 3개의 만족할만한 표는:

예1		예2		예3	
입력	출력	입력	출력	입력	출력
00	00	00	01	00	00
01	01	01	00	01	10
10	11	10	10	10	01
11	10	11	11	11	11

예의 표에 의해 제공된 단순한 치환의 효과를 역으로 할 수 없는 단순한 XOR이 상기로부터 보여질 수 있다. 본 발명의 수행에서, 표준 DES S-Box는 상보성을 갖지 않은 비선형 함수를 제공하기 위해 사용될 수 있다.

FIPS Pub. 46에서 발표된 데이터 암호화 표준은 4행 16열로 제공된 64값의 매트릭스를 각각 구성하는 상기 여러가지 8개의 근본 함수(즉, 치환박스;S1, … S8)에 실시된다. 이들 매트릭스(S-Box S_1)중 처음 하나는 아래와 같이 재현된다.:

S_1															
14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

이러한 S-Box는 4비트 출력(0과 15 사이의 값)을 제공하기 위한 6비트 입력(매트릭스에서 64개 엔트리중 하나)으로 어드레스된다. 하나는 S-Box 값의 16을 내포하는 각 페이지에서 4비트의 2비트 페이지된 조사처럼 S-Box를 보일 수 있었다. S-Box당 각 4페이지가 XOR동작에 의해 역으로되지 않는 특성을 유지하는 동안, 그들의 어느 것은 본 발명을 수행하는데 비선형 함수처럼 사용될 수 있었다. 상기(S_1) 묘사된 S-Box는 이 바람직한 특성을 갖는다. 이것은 테이블 그 자체를 시험하는 것에 의해 증명될 수 있다. 예컨대, 0에트리(1110처럼 표현된 14개의 값)와 15엔트리(0111에 의해 표현된 7개의 값)는 7엔트리(1000에 의해 표현된 8개의 값)의 XOR과 18엔트리(0011에 의해 표현된 3개의 값)처럼 같지 않다.

S-Box가 이미 DES 프로세서에 미리 저장됨에 따라, 제2도에 도시된 함수(20,22와/또는 24)를 제공하기 위해 그의 페이지를 사용하는 것이 효과적이다. 물론, 상보성을 갖지 않는 요구에 응하는 어떤 다른 조사 테이블 또는 논리함수가 대신에 사용될 수 있다.

본 발명에 사용된 암호화 알고리즘(예컨대, DES)의 암호화 강도를 줄이는 소정의 가능성을 피하기 위해, 함수(20,22 및/또는 24)가 암호화 동작전, 또는 암호화 동작 후, 또는 둘다에 배치되는 것이 필요하다. 제2도에 도시된 것 처럼, 실제 입력 키와 암호화 동작에 의해 사용된 키 사이의 함수를 배치시키는 것은 균등하게 타당하고, 키의 일대일 치환에 균일하다. 본 실시예에 있어서, 상보성이 없는 함수는 데이터 스트림 X와 암호화 프로세서의 출력에 부과하여 실제의 입력 키에 제공되고, 예측할 수 없는 키-독립 작용이 상보성 없이 발생되어 시스템의 강도를 최대로 한다.

본 발명에서는 상보특성 없이 DES와 같은 암호화 알고리즘을 수행하기 위한 구조이다. 상보성 없는 함수는 실제의 DES(또는 다른 암호화)처리 즉 외부에 제공한다. 함수는 암호화처리에 암호화 처리 후, 암호화처리 이전에, 및/또는 입력되는 보안성 키에 제공될 수 있다.

한편, 본 발명은 상기 실시예에 한정되는 것은 아니고, 다양하게 변형하여 실시할 수 있음은 물론이다.

(57) 청구의 범위

청구항 1.

데이터 블륵을 수신하기 위한 제1입력 포트와, 암호화 키를 수신하기 위한 제2입력 포트 및, 상기 키를 기초로 알고리즘에 의한 처리 후 상기 데이터 블록을 출력하기 위한 출력 포트를 포함하고, 상기 데이터 블록에 보안성 알고리즘을 공급하기 위한 암호화 수단과; 상기 암호화 수단의 외부로 상보성을 갖지 않는 함수를 인가하기 위한 상기 포트중 적어도 하나에 결합된 수단을 구비하여 이루어진 것을 특징으로 하는 상보특성을 갖는 블록 보안성 알고리즘을 이용하여 안전한 데이터 통신을 제공하기 위한 장치.

청구항 2.

제1항에 있어서, 상기 함수를 인가하기 위한 상기 수단이 조사 테이블로 이루어진 것을 특징으로 하는 장치.

청구항 3.

제2항에 있어서, 상기 조사 테이블이 DES S-Box로부터 추출되는 것을 특징으로 하는 장치.

청구항 4.

제1항에 있어서, 상기 함수를 인가하기 위한 상기 수단이 상기 제1입력 포트에 결합되는 것을 특징으로 하는 장치.

청구항 5.

제1항 있어서, 상기 함수를 인가하기 위한 상기 수단이 상기 제2입력 포트에 연결되는 것을 특징으로 하는 장치.

청구항 6.

제1항에 있어서, 상기 함수를 인가하기 위한 상기 수단이 상기 출력 포트에 연결되는 것을 특징으로 하는 장치.

청구항 7.

제1항에 있어서, 상보성 없이 함수가 상기 제1과 제2입력 포트의 각각에 인가되는 것을 특징으로 하는 장치.

청구항 8.

제7항에 있어서, 상보성 없이 동일 함수가 상기 제1과 제2입력 포트에 인가되는 것을 특징으로 하는 장치.

청구항 9.

제7항에 있어서, 상기 제1입력 포트에 인가되는 상보성이 없는 함수가 상기 제2입력 포트에 인가되는 상보성이 없이 함수와 다른 것을 특징으로 하는 장치.

청구항 10.

제1항에 있어서, 상보성이 없는 함수가 상기 제1입력 포트 및 상기 출력 포트의 각각에 인가되는 것을 특징으로 하는 장치.

청구항 11.

제10항에 있어서, 상보성이 없는 동일 함수가 상기 제1입력 포트 및 상기 출력 포트에 인가되는 것을 특징으로 하는 장치.

청구항 12.

제10항에 있어서, 상기 제1입력 포트에 인가된 상보성이 없는 함수가 상기 출력 포트에 인가된 상보성이 없이 함수와 다른 것을 특징으로 하는 장치.

청구항 13.

제1항에 있어서, 상보성이 없는 함수가 상기 제2입력 포트와 상기 출력 포트의 각각에 인가되는 것을 특징으로 하는 장치.

청구항 14.

제13항에 있어서, 상보성이 없이 동일 함수가 상기 제2입력 포트와 상기 출력 포트에 인가되는 것을 특징으로 하는 장치.

청구항 15.

제13항에 있어서, 상기 제2입력 포트에 인가된 상보성이 없는 함수가 상기 출력 포트에 인가된 상보성 없는 함수와 다른 것을 특징으로 하는 장치.

청구항 16.

제1항에 있어서, 상보성이 없는 함수가 상기 포트의 각각에 공급되는 것을 특징으로 하는 장치.

청구항 17.

제16항에 있어서, 상보성이 없는 동일 함수가 상기 포트중 2개에 인가되는 것을 특징으로 하는 장치.

청구항 18.

제16항에 있어서, 상보성이 없는 다른 함수가 상기 포트중 적어도 2개에 인가되는 것을 특징으로 하는 장치.

청구항 19.

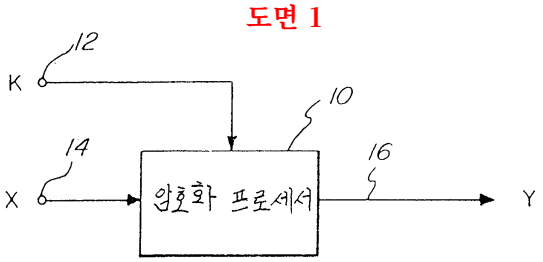
제1항에 있어서, 상보성을 갖고 있지 않은 상기 함수가 비선형인 것을 특징으로 하는 장치.

청구항 20.

상기 제19항에 있어서, 상기 블록 보안성 알고리즘이 데이터 암호화 표준(DES) 알고리즘으로 이루어진 것을 특징으로 하는 장치.

도면

도면 1



도면 2