(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl.[7]
H04L 9/22
G09C 1/00

(11) 공개번호 10-2004-0100850
(43) 공개일자 2004년12월02일

(21) 출원번호 10-2003-7016399
(22) 출원일자 2003년12월15일
번역문 제출일자 2003년12월15일
(86) 국제출원번호 PCT/JP2003/004915
(87) 국제공개번호 WO 2003/090185
(86) 국제출원출원일자 2003년04월17일
(87) 국제공개일자 2003년10월30일

(30) 우선권주장 JP-P-2002-00118509 2002년04월19일 일본(JP)

(71) 출원인 소니 가부시끼 가이샤
일본국 도쿄도 시나가와쿠 키타시나가와 6쵸메 7반 35고

(72) 발명자 마쓰다히로미
일본국 도쿄도 시나가와쿠 키타시나가와 6쵸메 7반 35고 소니 가부시끼 가이샤내

모리나가에이이치로
일본국 도쿄도 시나가와쿠 키타시나가와 6쵸메 7반 35고 소니 가부시끼 가이샤내

다나카마사오
일본국 도쿄도 시나가와쿠 키타시나가와 6쵸메 7반 35고 소니 가부시끼 가이샤내

(74) 대리인 박종길
김재만

심사청구 : 없음

(54) 키 생성 장치, 부호화 복호화 장치 및 키 생성 방법

요약

회로 설계자들이 키의 값을 용이하게 알 수 없어, 키의 보안이 지켜지는 키 생성 장치이다. 난수 발생 회로(51, 52, 53, …)에서 서로 별개의 클록(CLK1, CLK2, CLK3, …)에 의해 난수를 발생시킨다. 연산 회로(59)에서 난수 발생 회로(51, 52, 53, …)의 출력 난수를 연산하고, 난수 발생부(50)의 출력으로 하여 N 비트의 난수(RA)를 얻는다. 이 난수(RA)를 키 실렉터(43)를 통해 인출하고, 클록(CLK1, CLK2, CLK3, …)과는 다른 클록(CKLA)에 의해 구동되는 타이밍 감시 카운터(47)로부터의 획득 이네이블 신호(EN)에 의해 키 실렉터(45)에 래치하여, 고유의 비밀 키인 하드웨어 키를 얻는다.

대표도

도 1

색인어

키, 난수, 클록, 연산 회로, 연산.

명세서

기술분야

본 발명은 데이터의 암호화(부호화) 또는 복호화를 위한 비밀 키가 되는 키 데이터를 생성하는 키 생성 장치, 이 키 생성 장치를 구비하는 부호화 복호화 장치 및 키 생성 방법에 관한 것이다.

배경기술

기록 매체나 인터넷 등의 통신 네트워크에 의한 분배에 의해 PC(퍼스널 컴퓨터) 등의 단말에서, 암호화된 데이터를 수신하여, 예를 들면, 단말에 접속된 기록 재생 장치에 획득하고, 기록 재생 장치 내의 암호화 복호화 장치에서 복호화하여, 기록 매체에 기록하는 시스템이 고려되고 있다.

이 경우의 암호화 복호화 장치로서는, 도 4에 나타내는 바와 같은 장치가 고려된다. 암호화 복호화 처리부(60)는 IC(집적 회로)화되는 암호화 복호화 장치의 인터페이스나 CPU 등을 제외한 부분을 나타내며, 암호화 복호화 연산부(61), 키 실렉터(62), 하드웨어 키 생성부(64) 및 키 기억부(69)에 의해 구성된다.

하드웨어 키 생성부(64)는 고정값의 데이터가 기록된 ROM(65), 이 ROM(65)으로부터 판독된 데이터의 각 비트를 반전시키고, 시프트시켜 각 비트의 배타적 논리합(EOR ; XOR)을 산출하는 등, ROM(65)으로부터 판독된 데이터를 연산하는 연산 회 로(66), 및 외부로부터의 명령에 의해 지시된 타이밍으로, 클록(CLK)에 의해 연산 회로(66)의 출력 데이터를 래치하는 래치 회로(67)에 의해 구성되며, 래치 회로(67)의 출력 데이터가 하드웨어 키로서 키 실렉터(62)에 입력된다.

그리고 외부로부터의 명령에 의해, 최초에, 하드웨어 키 생성부(64)로부터의 하드웨어 키가 키 실렉터(62)에서 선택되고, 암호화 복호화 연산부(61)에서 입력 데이터와 연산되어 제1 단의 프로세스 키가 산출되고, 이것이 키 기억부(69)에 기록된다.

다음에, 이 키 기억부(69)로부터 판독된 제1 단의 프로세스 키가 키 실렉터(62)에서 선택되고, 암호화 복호화 연산부(61)에서 입력 데이터와 연산되어 제2 단의 프로세스 키가 산출되고, 이것이 제1 단의 프로세스 키에 대신하여 키 기억부(69)에 기록된다.

암호화 복호화 연산부(61)에서는, 이하, 동일하게 제3 단 이하의 프로세스 키가 산출되고, 최종적으로 데이터를 복원화 또는 암호화하기 위한 비밀 키인 컨텐츠 키가 산출되어 키 기억부(69)에 기록된다.

이 상태에서, 복호화 모드를 지시하는 명령이 입력되고, 입력 데이터로서 암호문 데이터가 입력되면, 키 기억부(69)로부터 판독된 컨텐츠 키가 키 실렉터(62)에서 선택되고, 암호화 복호화 연산부(61)에서 암호문 데이터와 연산되어 암호문 데이터가 복호화되고, 암호화 복호화 연산부(61)로부터 평문(平文) 데이터가 출력된다.

암호화 모드를 지시하는 명령이 입력되고, 입력 데이터로서 평문 데이터가 입력되는 경우에는, 동일하게, 평문 데이터가 암호화되어, 암호화 복호화 연산부(61)로부터 암호문 데이터가 출력된다.

그러나, 전술한 암호화 복호화 장치, 즉 암호화 복호화 처리부(60)에서는, 회로 설계자들은 회로도 상의 하드웨어 키 생성부(64)의 RTL(Register Transfer Level)에서의 기술(記述)을 봄으로써, 하드웨어 키의 값을 용이하게 알 수 있게 되어 버린다.

그러므로, 고유의 비밀 키로서의 하드웨어 키의 은닉성을 확보하기 위해, RTL에서의 설계 파일 관리에 세심한 주의를 기울이는 등의 필요가 있지만, 실제 상, 만전을 기하는 것은 곤란하기 때문에, 하드웨이 키의 은닉성을 확보하여 보안을 지키는 것이 어렵다.

그래서, 본 발명은 보안이 확실하게 지켜지도록 키 데이터를 생성할 수 있게 한 것이다.

발명의 상세한 설명

본 발명의 키 생성 장치는

각각 독립된 소정 주기로 난수(亂數)를 변화시켜 출력하는 복수의 난수 발생 수단과,

상기 복수의 난수 발생 수단으로부터 출력되는 각각의 난수가 입력되고, 입력된 상기 복수의 난수에 소정 연산 처리를 실행하여 키 정보를 생성하는 연산 처리 수단

을 구비하는 것으로 한다.

또 본 발명의 부호화 복호화 장치는

각각 독립된 소정 주기로 난수를 변화시켜 출력하는 복수의 난수 발생 수단과,

상기 복수의 난수 발생 수단으로부터 출력되는 각각의 난수가 입력되고, 입력되는 상기 복수의 난수에 소정 연산 처리를 실행하는 연산 처리부를 구비하는 키 생성 수단과,

입력되는 입력 데이터를 상기 키 생성 수단에서 생성되는 제1 키 정보에 따라 부호화 또는 복호화 처리를 실행하는 부호화 복호화 처리 수단

을 구비하는 것으로 한다.

또한 본 발명의 키 생성 방법은

각각 상이한 소정 주기로 난수를 복수 발생시키고,

상기 상이한 주기로 발생하는 복수의 난수에 소정 연산 처리를 실시하여 출력하는 것으로 한다.

상기 구성의 키 생성 장치, 부호화 복호화 장치 및 키 생성 방법에서는, 난수 발생 수단의 출력 데이터가 시계열(時系列)로 변화되므로, 회로도 상의 RTL에서의 기술을 본 것만으로는, 회로 설계자들도 래치 수단에 래치되는 실제의 키 데이터의 값을 알 수 없어, 키 데이터의 보안을 지킬 수 있다.

도면의 간단한 설명

도 1은 본 발명의 키 생성 장치의 한 실시예를 구비하는, 본 발명의 암호화 복화 장치의 한 실시예를 나타내는 도면이다.

도 2는 도 1의 키 생성 장치의 동작을 설명하기 위한 도면이다

도 3은 본 발명의 데이터 수신 장치의 한 실시예로서의 기록 재생 장치를 나타내는 도면이다.

도 4는 고려되는 키 생성 장치 및 암호화 복호화 장치의 예를 나타내는 도면이다.

실시예

[키 생성 장치 및 암호화 복호화 장치의 실시예 : 도 1 및 도 2]

도 1은 본 발명의 키 생성 장치의 한 실시예를 구비하는, 본 발명의 암호화 복호화 장치의 한 실시예를 나타낸다.

암호화 복호화 처리부(40)는 후술하는 바와 같이 IC화되는 암호화 복호화 장치의 인터페이스나 CPU 등을 제외한 부분을 나타내며, 하드웨어 키 생성부로서의 난수 발생부(50), 암호화 복호화 연산부(41), 키 실렉터(43), 키 저항기(45), 타이밍 감시용 카운터(47), 및 키 기억부(49)에 의해 구성된다.

난수 발생부(50)는 복수의 난수 발생 회로, 및 연산 회로(59)에 의해 구성된다. 도면에서는 3개의 난수 발생 회로(51 53)를 나타내지만, 실제 상으로는, 보다 다수의 난수 발생 회로가 설치된다.

난수 발생 회로(51)는 저항기(511) 및 연산 회로(512)에 의해 구성되고, 암호화 복호화 처리부(40)의 외부로부터 저항기(511)에 명령, 리셋 신호 및 클록(CLK1)이 입력되고, 연산 회로(512)에서 저항기(511)의 출력 데이터의 각 비트가 반전되어 시프트되고, 각 비트의 배타적 논리합이 산출되는 등 저항기(511)의 출력 데이터가 연산되고, 그 연산 후

의 데이터가 클록(CLK1)에 의해 저항기(511)에 기록된다고 하는 동작이 클록(CLK1)의 펄스마다 반복되어, 저항기(511)로부터 n 비트 길이의, 예를 들면, 8 비트 길이의, 클록(CLK1)의 펄스마다 변화되는 난수가 출력된다.

난수 발생 회로(52)는 저항기(521) 및 연산 회로(522)에 의해 구성되고, 클록(CLK1)과는 별개의 클록(CLK2)에 의해 난수 발생 회로(51)와 동일하게, 저항기(521)로부터 n 비트 길이의, 클록(CLK2)의 펄스마다 변화되는 난수가 출력되고, 난수 발생 회로(53)는 저항기(531) 및 연산 회로(532)에 의해 구성되고, 클록(CLK1, CLK2)과는 별개의 클록(CLK3)에 의해 난수 발생 회로(51, 52)와 동일하게, 저항기(531)로부터 n 비트 길이의, 클록(CLK3)의 펄스마다 변화되는 난수가 출력된다. 도면에서는 생략한 다른 난수 발생 회로에 대해서도 동일하다.

또한 난수 발생부(50)에서는, 연산 회로(59)에서 난수 발생 회로(51, 52, 53, …)의 출력 난수가 합성되어, 합계 N 비트의, 예를 들면, n=8이며, 또한 난수 발생 회로의 총수가 8 개인 경우에는 64 비트의 난수가 생성되는 동시에, 그 난수의 각 비트가 반전되어 시프트되고, 각 비트의 배타적 논리합이 산출되는 등 그 난수가 연산되어, N 비트의 난수(RA)가 얻어진다.

난수 발생 회로(51, 52, 53, …)의 출력 난수는 서로 별개의 클록(CLK1, CLK2, CLK3, …)에 의해 변화되므로, 이 난수 발생부(50)의 출력 난수(RA)는 도 2에 데이터(R1, R2, R3, R4, R5, …)로서 나타내는 바와 같이, 불규칙한 타이밍으로 변화하는 것이 된다.

이 난수 발생부(50)의 출력 난수(RA)는 키 실렉터(43)에 입력되고, 입력 명령에 의해 키 실렉터(43)가 제어됨으로써, 키 실렉터(43)에서 난수(RA)와, 후술하는 바와 같이 키 기억부(49)로부터 판독된 키 데이터 중 어느 하나가 선택되고, 그 선택된 데이터가 키 실렉터(45)에 입력된다.

한편, 타이밍 감시용 카운터(47)는 입력 명령 및 리셋 신호에 의해 리셋되고, 스타트 시점부터 상기 난수 발생용 클록(CLK1, CLK2, CLK3, …)과는 별개의 클록(CLKA)을 카운트하여, 소정 수를 카운트한 시점에서 획득 이네이블 신호(EN)를 출력한다.

그리고 키 저항기(45)에서는, 이 획득 이네이블 신호(EN)가 출력된 시점에서의 클록(CKLA)에 의해, 그 때의 키 실렉터(43)의 출력 데이터가 획득되어, 키 데이터로서 출력된다.

따라서, 키 실렉터(43)의 출력 데이터로서, 난수 발생부(50)의 출력 난수(RA)가 선택되는 경우에는, 도 2에 데이터(R1, R2, R3, R4, R5, …)로서 나타내는 바와 같이 불규칙한 타이밍으로 변화되는 난수(RA) 중의, 획득 이네이블 신호(EN)가 출력된 시점(ta)에서의 데이터(R3)가 키 저항기(45)에 래치되어, 하드웨어 키로서 출력된다.

암호화 복호화 연산부(41)에서는, 이와 같이 키 실렉터(43)에서 선택되어, 키 저항기(45)에 래치된 데이터가 키 데이터로서 입력 데이터와 연산되어 프로세스 키가 산출되고, 최종적으로 컨텐츠 키가 산출되는 동시에, 그 컨텐츠 키에 의해 DES(Data Encryption Standard)나 Triple DES 등의 암호 알고리즘에 의해 데이터가 복호화 또는 암호화된다.

구체적으로, 입력 명령에 의해, 최초에 키 실렉터(43)에서는 난수 발생부의 출력 난수(RA)가 선택되고, 이것이 전술한 바와 같이 키 저항기(45)에 래치되어, 키 저항기(45)의 출력 키 데이터로서 하드웨어 키가 얻어지고, 이것이 암호화 복호화 연산부(41)에서 입력 데이터와 연산되어 제1 단의 프로세스 키가 산출되고, 이것이 키 기억부(49)에 기록된다.

다음에, 이 키 기억부(49)로부터 판독된 제1 단의 프로세스 키가 키 실렉터(43)에서 선택되고, 키 저항기(45)에 래치되어 키 레지스터(45)의 출력 키 데이터로서 제1 단의 프로세스 키가 얻어지고, 이것이 암호화 복호화 연산부(41)에서 입력 데이터와 연산되어 제2 단의 프로세스 키가 산출되고, 이것이 제1 단의 프로세스 키에 대신하여 키 기억부(49)에 기록된다.

암호화 복호화 연산부(41)에서는, 이하, 동일하게 제3 단 이하의 프로세스 키가 산출되고, 최종적으로 컨텐츠 키가 산출되어 키 기억부(49)에 기록된다.

이 상태에서, 복호화 모드를 지시하는 명령이 입력되고, 입력 데이터로서 암호문 데이터가 입력되면, 키 기억부(49)로부터 판독된 컨텐츠 키가 키 실렉터(43)에서 선택되고, 키 저항기(45)에 래치되어 키 저항기(45)의 출력 키 데이터로서 컨텐츠 키가 얻어지고, 이것이 암호화 복호화 연산부(41)에서 암호문 데이터와 연산되어, 암호문 데이터가 복호화되고, 암호화 복호화 연산부(41)로부터 평문 데이터가 출력된다.

암호화 모드를 지시하는 명령이 입력되고, 입력 데이터로서 평문 데이터가 입력되는 경우에는, 동일하게, 평문 데이터가 암호화되어, 암호화 복호화 연산부(41)로부터 암호문 데이터가 출력된다.

전술한 키 생성 장치에서는, 난수 발생 회로(51, 52, 53, …)의 출력 데이터가 시계열로 변화되고, 또한 난수 발생부(50)의 출력 난수(RA)가 불규칙한 타이밍으로 변화되므로, 회로도 상의 RTL에서의 기술을 본 것만으로는, 회로 설계자들도 키 저항기(45)에 획득되는 실제의 하드웨어 키의 값을 알 수 없다. 따라서, 하드웨어 키의 보안이 지켜진다.

또한 장치 내의 각 저항기에 저항기명(名)으로서 난수명이 붙여지고, 하드웨어 키에 관한 모든 노드에서는, 비트마다 스크램블이 걸림으로써, 회로 설계자들은 장치 내의 저항기의 값을 읽었다고 해도, 진짜 하드웨어키의 값을 판독할 수 없어, 보안 강도가 한층 높아진다.

[데이터 수신 장치의 실시예 : 도 3]

도 3은 본 발명의 암호화 복호화 장치를 구비하는, 본 발명의 데이터 수신 장치의 한 실시예로서의 기록 재생 장치를 포함하는 데이터 수신 시스템을 나타낸다.

이 예의 데이터 수신 시스템에서는, 기록 매체(1)로부터의 리핑(ripping)이나, 인터넷을 이용한 분배 시스템(2)으로부터의 다운로드 등에 의해 PC 등의 단말(10)에서 부호화되고, 또한 비밀 키에 의해 암호화된 데이터가 수신된다.

그 수신된 암호문 데이터는 단말(10)로부터 단말(10)의 USB(Universal Serial Bus) 단자에 접속된 기록 재생 장치(20)에 송신된다.

기록 재생 장치(20)는 기록 매체(5) 상에 데이터를 기록하고, 기록 매체(5) 상으로부터 데이터를 재생하는 것으로, 이것에 암호화 복호화 장치(30)가 설치된다.

암호화 복호화 장치(30)는 도 1에 나타낸 전술한 암호화 복호화 처리부(40)를 구비하는 외에, CPU(31)를 구비하고, 그 버스(32)에 CPU(31)가 실행해야 할 명령 송수(送受)나 암호화 복호화 처리 등의 프로그램이나 필요한 고정 데이터 등이 기록된 ROM(33), CPU(31)의 워크 영역 등으로서 기능하는 RAM(34), 단말(10) 사이에서 명령을 송수하고, 단말(10)로부터 데이터를 획득하는 USB 인터페이스(36), 기록 재생 장치 본체부의 DSP(Digital Signal Processor)(26)에 데이터를 출력하기 위한 인터페이스(37), 및 기록 재생 장치 본체부의 CPU(21) 사이에서 명령을 송수하기 위한 인터페이스(39)가 접속된다.

이 암호화 복호화 장치(30)는 단일 칩 LSI(대규모 집적 회로)로서 형성된다.

기록 재생 장치 본체부는 CPU(21)의 버스(22)에, CPU(21)가 실행해야 할 프로그램이나 필요한 고정 데이터 등이 기록된 ROM(23), CPU(21)의 워크 영역 등으로서 기능하는 RAM(24), 및 상기 DSP(26)가 접속되고, DSP(26)에 기록 재생 처리부(27), 및 출력 처리부(28)가 접속된다.

암호화 복호화 장치(30)에서는, USP 인터페이스(36)를 통해 단말(10)로부터 획득되어 부호화되고, 또한 비밀 키에 의해 암호화된 데이터가 암호화 복호화 처리부(40)에서, 전술한 바와 같이 컨텐츠 키에 의해 복호화되고, 그 복호화된 평문 데이터로서의, 부호화된 데이터가 인터페이스(37)를 통해 DSP(26)에 송출되고, DSP(26)에서 처리된 후, 기록 재생 처리부(27)에 의해 기록 매체(5) 상에 기록되고, 또는 출력 처리부(28)에 의해 아날로그 신호로 변환되어 출력 단자(29)로 도출된다.

기록 매체(5)로서는, 광 디스크, 하드 디스크, 플렉시블 디스크, 자기 테이프, 메모리 카드, 반도체 메모리 등 어느 것이라도 된다.

또 이와 같은 기록 재생 장치에 한정되지 않고, 암호화된 데이터를 수신하여 복호화하고, 재생하는 것만으로 기록 기능을 구비하지 않은 장치에도 본 발명을 적용할 수 있다.

전술한 바와 같이, 본 발명에 의하면, 키 데이터의 보안을 확실하게 지킬 수 있다.

(57) 청구의 범위

청구항 1.

각각 독립된 소정 주기로 난수(亂數)를 변화시켜 출력하는 복수의 난수 발생 수단과,

상기 복수의 난수 발생 수단으로부터 출력되는 각각의 난수가 입력되고, 입력된 상기 복수의 난수에 소정 연산 처리를 실행하여 키 정보를 생성하는 연산 처리 수단

을 구비하는 키 생성 장치.

청구항 2.
제1항에 있어서,

상기 난수 발생 수단은 각각

입력되는 입력 데이터에 소정 처리를 실행하여 출력하는 데이터 연산 수단과,

상기 데이터 연산 수단의 출력 데이터를 상기 난수 발생 수단마다 독립하여 주어지는 획득(acquisition) 지시에 따라 획득하여 유지하고, 상기 지시에 따라 유지된 출력 데이터를 상기 데이터 연산 수단에 입력하는 데이터 유지 수단

을 구비하는 키 생성 장치.

청구항 3.
제2항에 있어서,

상기 데이터 연산 수단은 입력되는 입력 데이터의 비트열(列)에 대해 비트 반전 처리, 시프트 처리, 배타적 논리합 처리 중 적어도 하나를 실행하는 키 생성 장치.

청구항 4.
제1항에 있어서,

상기 난수 발생 수단으로부터 출력되는 난수의 데이터 길이보다 상기 연산 처리 수단에서 생성되는 키 정보의 데이터 길이가 긴 키 생성 장치.

청구항 5.
각각 독립된 소정 주기로 난수를 변화시켜 출력하는 복수의 난수 발생 수단과,

상기 복수의 난수 발생 수단으로부터 출력되는 각각의 난수가 입력되고, 입력되는 상기 복수의 난수에 소정 연산 처리를 실행하는 연산 처리부를 구비하는 키 생성 수단과,

입력되는 입력 데이터를 상기 키 생성 수단에서 생성되는 제1 키 정보에 따라 부호화 또는 복호화 처리를 실행하는 부호화 복호화 처리 수단

을 구비하는 부호화 복호화 장치.

청구항 6.
제5항에 있어서,

상기 난수 발생 수단은 각각

입력되는 입력 데이터에 소정 처리를 실행하여 출력하는 데이터 연산 수단과,

상기 데이터 연산 수단의 출력 데이터를 상기 난수 발생 수단마다 독립하여 주어지는 획득 지시에 따라 획득하여 유지하고, 상기 획득 지시에 따라 획득되어 유지된 출력 데이터를 상기 데이터 연산 수단에 입력하는 데이터 유지 수단

을 구비하는 부호화 복호화 장치.

청구항 7.
제5항에 있어서,

상기 부호화 복호화 장치는

입력되는 입력 데이터를 제2 키 정보로서 유지하는 키 유지 수단과,

상기 키 생성 수단에서 생성되는 제1 키 정보와, 상기 키 유지 수단에 유지된 제2 키 정보를 선택하여 출력하는 키 선택 수단을 추가로 구비하고,

상기 부호화 복호화 처리 수단은 상기 키 선택 수단에서 선택된 키 정보에 따라 부호화 또는 복호화 처리를 실행하는 부호화 복호화 장치.

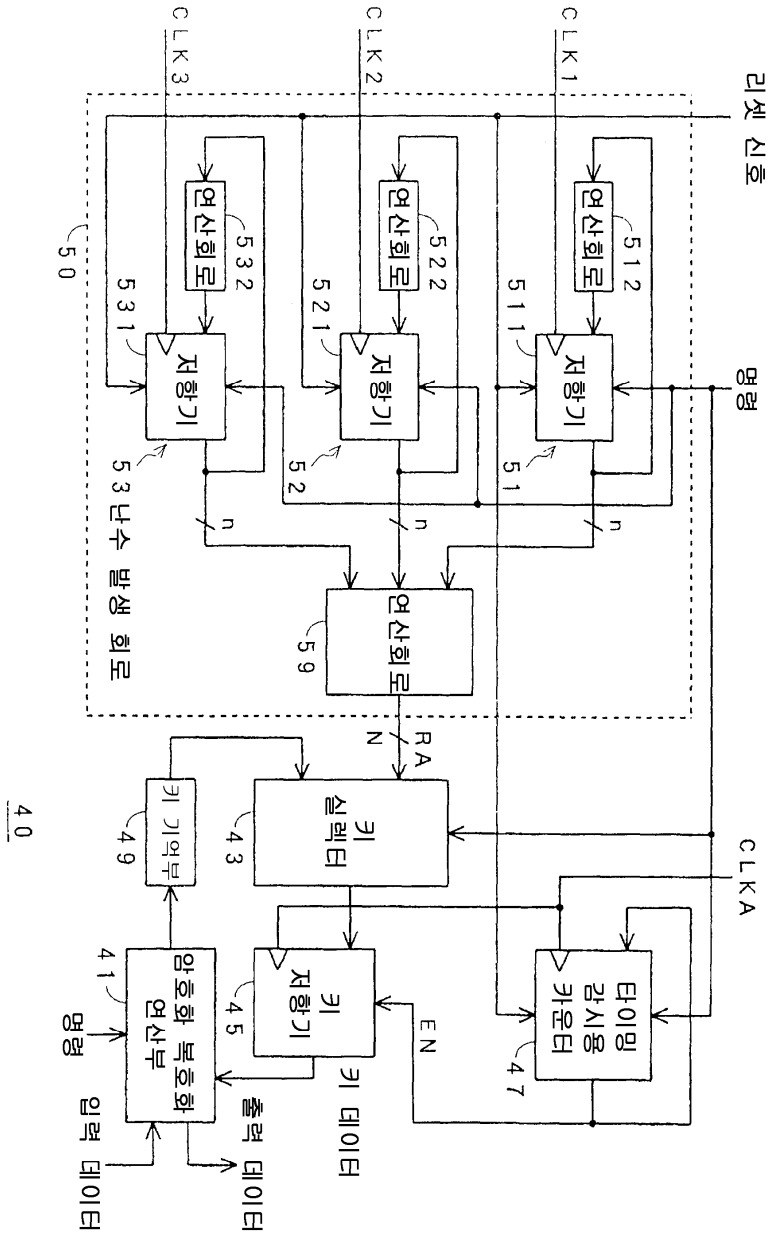
청구항 8.

각각 상이한 소정 주기로 난수를 복수 발생시키고,

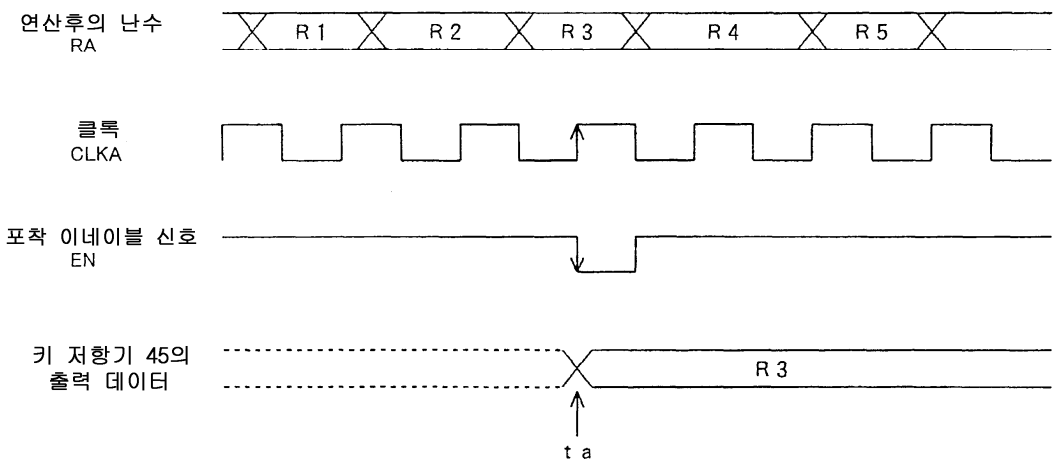
상기 상이한 주기로 발생하는 복수의 난수에 소정 연산 처리를 실시하여 출력하는 키 생성 방법.

도면

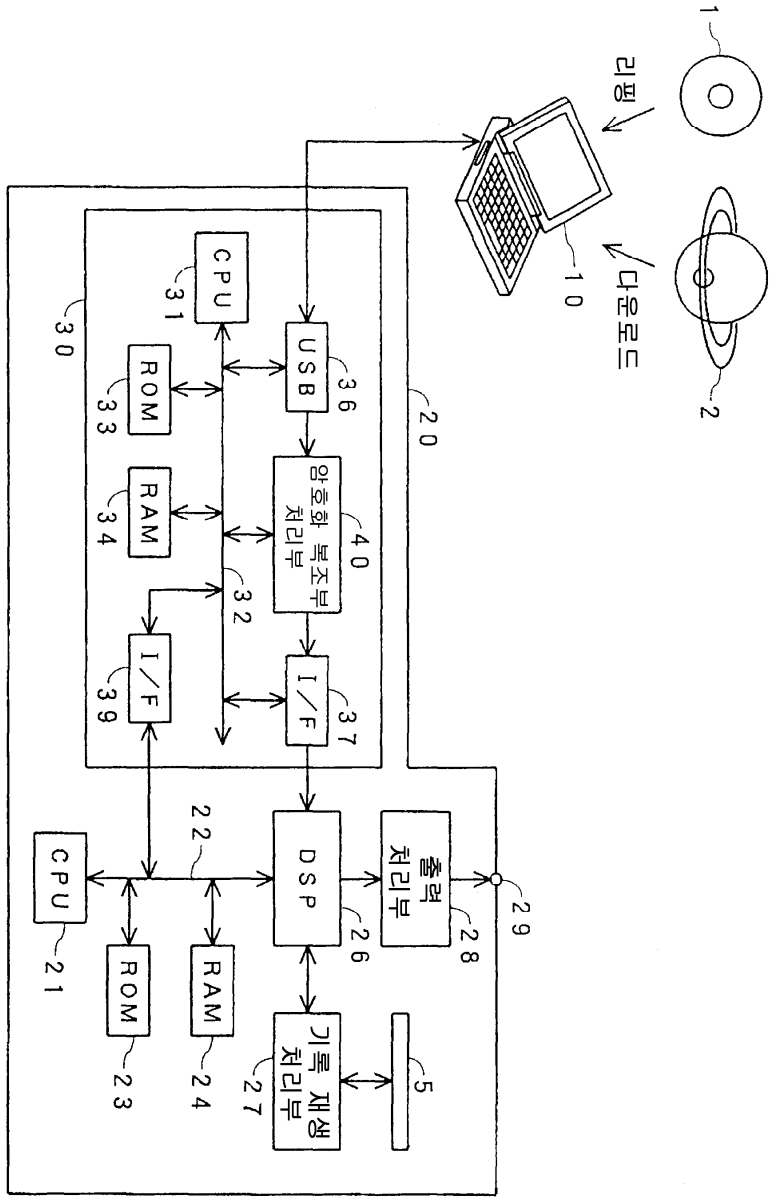
도면1



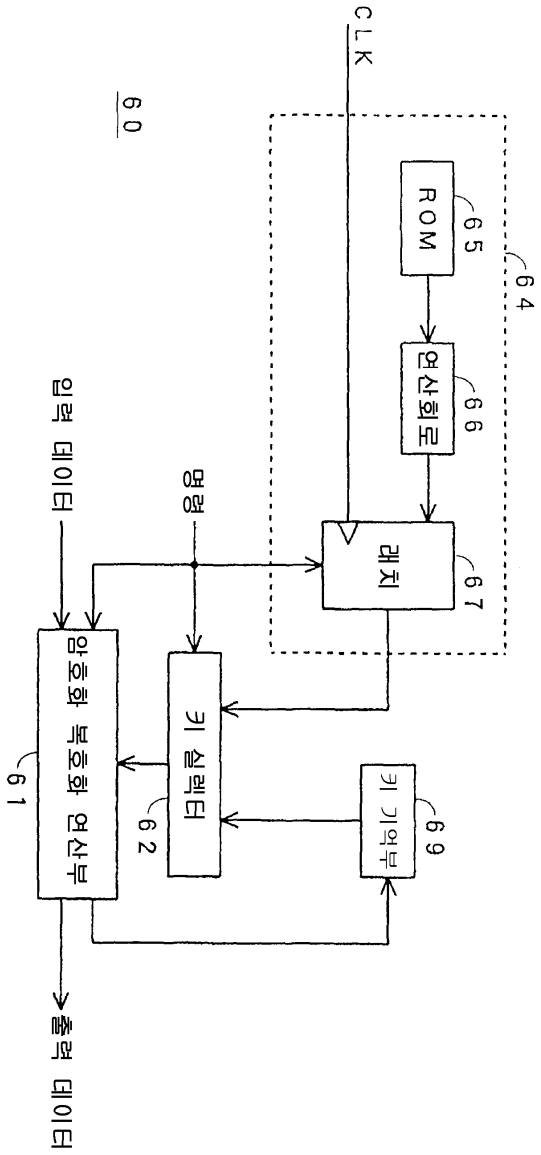
도면2


연산후의 난수
RA
R1
R2
R3
R4
R5
클록
CLKA
포착 이네이블 신호
EN
키 저항기 45의
출력 데이터
R3
t a

도면3


1
리핑
10
다운로드
2
20
30
CPU
31
USB
36
ROM
33
RAM
34
암호화 복조부
40
32
I/F
39
I/F
37
CPU
21
22
DSP
26
출력
처리부
28
29
ROM
23
RAM
24
기록 재생
처리부
27
5

도면4


CLK
60
ROM
65
64
연산회로
66
입력 데이터
명령
래치
67
암호화 복호화 연산부
61
키 셀렉터
62
키 기억부
69
출력 데이터