



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2007-0109154
(43) 공개일자 2007년11월15일

(51) Int. Cl.

G06F 7/58 (2006.01) G06F 7/70 (2006.01)

(21) 출원번호 10-2006-0041730

(22) 출원일자 2006년05월10일

심사청구일자 2006년05월10일

(71) 출원인

동서대학교산학협력단

부산광역시 사상구 주례2동 산69-1 동서대학교

(72) 발명자

조상일

경남 김해시 진영읍 여래리 장복아파트 202동 1205호

김봉근

부산 금정구 구서1동 563-40 금강부광아파트 101-310

이훈재

부산 사상구 주례2동 80-84번지 4동 201호

전체 청구항 수 : 총 4 항

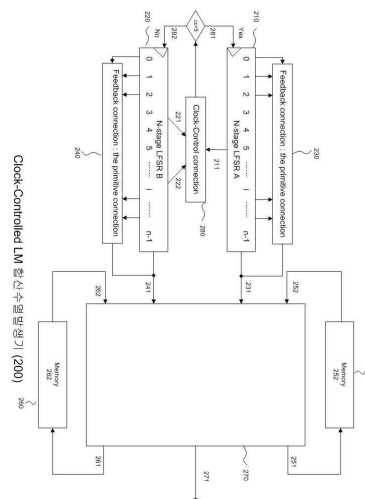
(54) 암호시스템에 사용하기 위한 클럭 조절 함수를 이용한 키스트림 생성 방법

(57) 요약

선형 피드백 시프트레지스터(LFSR)의 클럭 조절을 사용하여 랜덤 키스트림을 생성하는 장치 및 방법이 개시되어 있다.

상기 장치의 클럭 조절부는 n개의 LFSR의 비트들로 구성되며, 클럭 조절 함수에 의해 n개의 LFSR 비트들이 연산되며, 연산된 결과 값에 의해 암호 시스템의 LFSR의 클럭을 조절하게 된다. 상기의 LFSR의 피드백된 값은 2개의 메모리 함수 값과 XOR 연산의 통해 암호시스템의 키스트림의 비트들로서 출력한다.

대표도 - 도2



특허청구의 범위

청구항 1

암호시스템에 사용하기 위한 2개 이상의 LFSR을 사용하는 방식에 있어서, 클럭 콘트롤 하기 위한 클럭의 연산을 위한 부분(280)이 있으며, 계산을 하기 위한 비교 부분을 포함하며, 피드백된 비트(231과 241)의 메모리 비트(252와 262)를 포함하며 각각의 연산을 통해 최종 출력 비트를 생성을 특징으로 상기 장치.

청구항 2

제 1항에 있어서, 상기 클럭 콘트롤의 클럭을 연산하기 위한 다항식을 구성됨을 특징으로 하는 상기 장치

청구항 3

제 1항에 있어서, 상기 클럭 콘트롤 비교를 위해 다항식 출력 결과를 비교하는 부분을 구성됨을 특징

청구항 4

제 1항에 있어서, 상기 서브 저장부들은 동일한 수의 저장 스테이지들로 구성됨을 특징으로 하는 상기 장치.

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

- <4> 본 발명은 암호시스템에 관한 것으로, 특히 선형피드백 시프트레지스터(LFSR)의 클럭 조절을 사용하여 입력 정보의 암호화를 위한 랜덤 키스트림을 생성하는 방법에 관한 것이다.
- <5> 최근 통신망의 급격한 발전과 더불어 처리할 데이터도 텍스트/음성 데이터에서 화상회의나 동영상 자료 등 점차 멀티미디어 자료 형태로 변모해가고 있다. 이에 따라 통신 시스템에서 사용되는 암호 알고리즘도 고비도, 고속화 및 고신뢰도 설계가 요구되고 있다.
- <6> 일반적으로 암호 방식은 스트림 암호(stream cipher), 블록 암호(block cipher) 그리고 공개키 암호(public key cipher)로 분류될 수 있다. 상기 블록 암호는 적용 방식에 따라 ECB(Electronic CodeBook) 모드, CFB(Cipher FeedBack) 모드, CBC(Cipher Block Chaining) 모드 및 OFB(Output FeedBack) 모드로 구분된다. 상기 ECB 모드는 블록 크기의 입력에 대하여 비밀키(Secret Key)와 DES(Data Encryption Standard) 함수로부터 블록 출력을 생성하는 방식이다. 상기 CFB 모드는 출력 암호문을 입력에 피드백(feedback)시킨다. 상기 CBC 모드는 송수신 데이터 인증을 위
- <7> 하여 현재 암호문 블록과 다음 번 평문 블록을 배타적논리합(XOR: exclusive-OR) 연산시킨 후 블록 암호에 입력시켜 새로운 출력을 생성하고, 이 출력을 다시 그 다음 번 입력과 XOR시키는 반복 과정으로 최종 인증 값을 얻는 방식이다. 이러한 CBC 모드는 데이터 위조시 최종 인증 값이 바뀌게 되므로 진위 구별이 가능하다. 상기 OFB 모드는 블록 암호 자체를 랜덤 스트림 발생기(random stream generator)로 변경하여 스트림 암호처럼 적용시킨다.
- <8> 상기 4가지 방식들의 블록 암호는 모두 실제 암호 통신을 하는 실용화 측면에서 채널 에러에 대부분 취약하거나 또다른 문제점을 안고 있기 때문에 어떤 대 책이 요구된다. 구체적으로 말하면, 상기 ECB 모드에서는, 하나의 암호문 블록에서의 하나 또는 그 이상의 비트 에러들은 단지 그 블록의 해독에 영향을 미친다. 상기 CFB 모드에서는, 하나의 암호문 블록에서의 하나의 비트 에러는 그 블록과 다음 블록의 해독에 영향을 미친다. 상기 CBC 모드에서는, 하나의 암호문 블록에서의 하나의 비트 에러는 이후 모든 블록들에 영향을 미친다. 블록 암호의 에러 확산을 줄이기 위하여 도입된 OFB 모드는 입력 피드백 비트 수(이 수는 블록 크기보다 작음)만큼 확산을 줄일 수 있으며, 최상의 경우 1비트를 피드백시켜 근본적으로 확산을 방지할 수 있다. 하지만 1비트 크기의 OFB 모드는 일반 ECB 모드보다는 데이터 처리 속도가 블록 크기 배 감소되기 때문에 오히려 통신망 처리 능력을 떨어뜨린다.

- <9> 또한, 공개키 암호는 처리 속도가 느리기 때문에 고속 데이터 처리에 부적합할 뿐 아니라 ECB 모드처럼 에러가 블록 전체로 확산되는 단점이 있다. 또한, 스트림 암호는 채널 에러 확산이 없고 안전성(비도 수준) 요소가 몇 가지 측면에서 수학적으로 보장이 되며 고속 처리가 가능한 장점이 있지만, 이 방법 역시 초고속 통신 서비스에 따른 암호 처리를 원활하게 할 수 있을지는 의문이다.
- <10> 한편, 스트림 암호를 구현시에 많이 사용되는 소자로 선형피드백 시프트레지스터(LFSR: Linear Feedback Shift Register)와 비선형 결합함수형태의 논리조합회로, 전가산기(full adder), 멀티플렉서(multiplexer) 등을 들 수 있다. 특히 LFSR은 크기의 다양성 뿐만 아니라 키 수열의 주기라는 비도 요소를 결정짓기 때문에 암호시스템에서는 거의 필수적으로 사용되고 있는 소자이다. 상기 LFSR은 도 1에 도시된 바와 같이 외부에서 입력되는 시스템 클럭에 맞추어 동기적으로 1비트씩 이동시키면서 이진 키 스트림(key stream)을 발생한다. 상기 발생된 키 스트림은 암호화 결합기(Encryption Combiner)로 제공되어 평문(plain text)을 암호문(Cipher Text)으로 변환하는데 이용된다. 이때 상기 키 스트림의 발생 속도는 시스템 클럭과 내부 회로의 지연시간에 의해서 결정된다.
- <11> 전술한 도 1에 도시된 바와 같은 LFSR은 의사잡음(Pseudo Noise) 부호의 생성이나 암호화를 위한 처리에서 필수적으로 사용되는 소자이다. 특히 암호화되어야 할 대상이 멀티미디어 서비스를 위한 데이터로 점차적으로 변화되고 있는 추세에 비추어볼 때 고비도의 LFSR 처리가 필요하다. 그러나 종래 기술에 따른 LFSR 구조는 한 시스템 클럭에 한 비트씩의 이동만을 가능하게 하며, 이러한 점은 LFSR의 구조를 분석을 쉽게 할 수 있다는 구조를 가지고 있다고 할 수 있다.

발명이 이루고자 하는 기술적 과제

- <12> 따라서 본 발명의 목적은 암호시스템 혹은 확산 스펙트럼 통신시스템에서 사용하기 위한 랜덤 키스트림을 고속으로 생성하는 방법을 제공함에 있다.
- <13> 본 발명의 다른 목적은 LFSR의 선형적인 구조에 의해 암호 공격자의 LFSR의 구조 파악을 어렵게 하는 방법을 제공함에 있다.
- <14> 이러한 목적들을 달성하기 위한 본 발명은 하나의 시스템 클럭내에서 LFSR을 m클럭씩 이동이 가능하게 2개 이상의 LFSR을 사용하는 키스트림 생성 방법에서의 고비도의 키스트림을 생성하는 키스트림 생성 방법을 제안한다. 상기 장치의 LFSR은 LFSR 210과 LFSR 220의 저장된 비트 값에서 Clock-control connection 280 부분으로 비트값을 연산으로 통해 Clock-control 281 값이 생성된다.
- <15> 상기 방법에서 생성된 값(281)은 비교를 통해 LFSR 210과 LFSR 220의 클럭을 조절하게 되며, 이러한 클럭 조절을 통해 피드백 되는 값(231, 241)과 메모리 함수 값(252, 262)값들과의 연산을 통해 키스트림 비트 값을 출력한다.

발명의 구성 및 작용

- <16> 이하 본 발명의 바람직한 실시예의 상세한 설명이 첨부된 도면들을 참조하여 설명될 것이다. 도면들 중 참조번호들 및 동일한 구성요소들에 대해서는 비록 다른 도면상에 표시되더라도 가능한 한 동일한 참조번호들 및 부호들로 나타내고 있음에 유의해야 한다. 하기에서 본 발명을 설명함에 있어, 관련된 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다.
- <17> 하기에서 본 발명은 암호시스템의 초고속화와 공격자의 LFSR 구조를 분석을 어렵게 하는 암호 시스템의 설계라는 두 가지 목적들 하에서에서, 스트림 암호의 LFSR을 클럭 조절과 클럭의 제한을 둠으로써 랜덤 키스트림을 생성하는 방법을 제안한다.
- <18> 즉, 본 발명의 실시예는 스트림 암호의 비도 수준을 증가와 고속 상태를 유지 시킴으로써 초고속, 고비도의 처리가 가능하게 한다. LFSR은 한 클럭에 1비트씩 이동되는데 이를 개선한 본 발명은 클럭을 조절함으로써 1~4회의 클럭을 이동이 가능하다. 또한 본 발명은 두 개이상의 LFSR 클럭 조절에서 클럭의 최대 실행 수의 제한을 둠으로써 고속의 랜덤 키스트림 생성이 가능하게 제안한다.
- <19> 도 2는 본 발명의 실시예에 따른 LFSR의 클럭을 조절하게 되는 랜덤 키스트림을 생성하는 방법의 블록 구성도이다.

- <20> 상기 도 2를 참조하면, 키스트림 생성 장치는 LFSR A 210과 LFSR B 220, 메모리 저장비트 250, 260과 출력 비트 연산 270을 포함한다.
- <21> 상기 LFSR A 210과 LFSR B 220은 Feedback connection 230, 240에 의해 각각 비트의 값을 피드백시키게 되며, LFSR A와 LFSR B의 비트 상태에 의해 Clock-Control Connection 280의 연산을 통해 클럭 콘트롤 하게 된다.
- <22> 도 3을 통해 클럭 콘트롤 구분을 자세히 보면 LFSR A 310와 LFSR B 320의 각각의 비트값 311은 LFSR A의 64번째 비트의 값이며, 321은 LFSR B의 42번째 비트의 값이며 322는 LFSR B의 85번째 비트의 값을 추출하여 다음과 같이 다항식 $381 = 4s311 + 2s321 + 322$ 을 이용해 연산을 수행하게 된다.
- <23> 상기 클럭 콘트롤 다항식에 의해 얻어진 값 cc는 cc의 값의 비교를 통해 LFSR A 310와 LFSR B 320의 클럭을 조절하게 된다. cc의 값이 5보다 낮은 경우(no) 1~4번 LFSR B 320을 cc 값에 의해 클럭을 움직이게 된다. 이때, LFSR A 310은 1회 클럭을 움직이게 된다. 만일 cc의 값이 5보다 높을 경우(yes) cc의 값에서 4의 값을 차감한 값(1~4) 만큼 LFSR A 310의 클럭을 움직이게 된다. 이때, LFSR B 320은 1회 클럭을 움직이게 된다.
- <24> 상기와 같이 클럭 조절의 통해 LFSR A 210과 LFSR B 220의 클럭이 이동하게 되면 Feedback connection 230과 240을 통해 피드백 값 231과 241이 생성되게 된다.
- <25> 상기에서 주의할 사항으로는 LFSR A와 LFSR B의 값이 동시에 1~4 만큼의 클럭을 이동하는게 아니며 cc의 값의 크기에 의해 LFSR A210와 LFSR B220 둘 중 한 곳에만 클럭 조절이 된다는 점이다.
- <26> 상기 피드백 되는 값 231과 241을 값을 생성하기 위해 231은 다항식 $231 = x^{127} \cup x^{107} \cup x^{10} \cup x^9 \cup x^7 \cup x^6 \cup x^5 \cup x^4 \cup x^3 \cup x^2 \cup 1$ 에 의해 연산이 되며, 241은 다항식 $241 = x^{129} \cup x^{117} \cup x^{14} \cup x^{11} \cup x^{10} \cup x^9 \cup x^8 \cup x^7 \cup x^6 \cup x^5 \cup x^4 \cup x^3 \cup x^2 \cup x^1 \cup 1$ 에 의해 연산된다. 상기 2개의 메모리 비트 함수 252는 다항식 $252 = 231s241 \cup (231 \cup 241) \cup 251$ 에 의해 연산이 되며 메모리 비트 함수 262는 다항식 $262 = 241 \cup (231 \cup 241) s261$ 에 의해 연산이 되어 메모리 비트를 저장하게 된다. 생성된 값 231과 241의 값은 메모리 비트에 저장된 비트 252와 262 값과 같이 연산을 통해 최종 출력 비트 271을 출력한다.
- <27> 상기 271의 비트를 출력하기 위해 다항식 $271 = 231 \cup 241 \cup 252 \cup 262$ 연산을 통해 최종 출력 비트 271을 출력 한다. 상기에서 최종 출력 비트 271 값은 암호화 처리를 위한 1비트의 키스트림으로서 생성된다.

발명의 효과

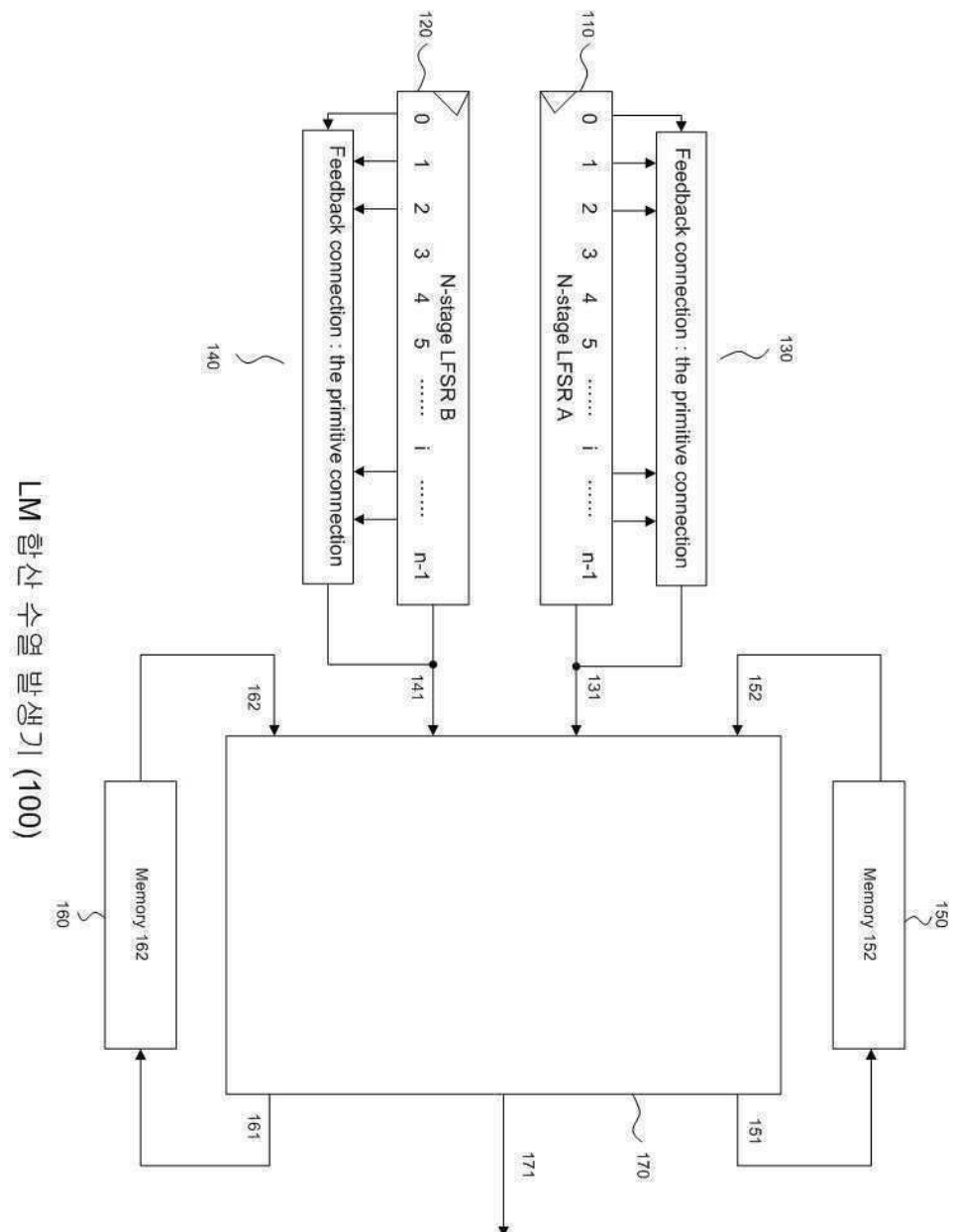
- <28> 상술한 바와 같이 본 발명은 고속의 동작하는 LFSR의 클럭 조절을 통해 암호 시스템의 비도를 향상 시킬 수 있으며 클럭의 제한을 통해 키스트림의 생성 시간이 늘어 나지 않도록 하는 이점이 있다.

도면의 간단한 설명

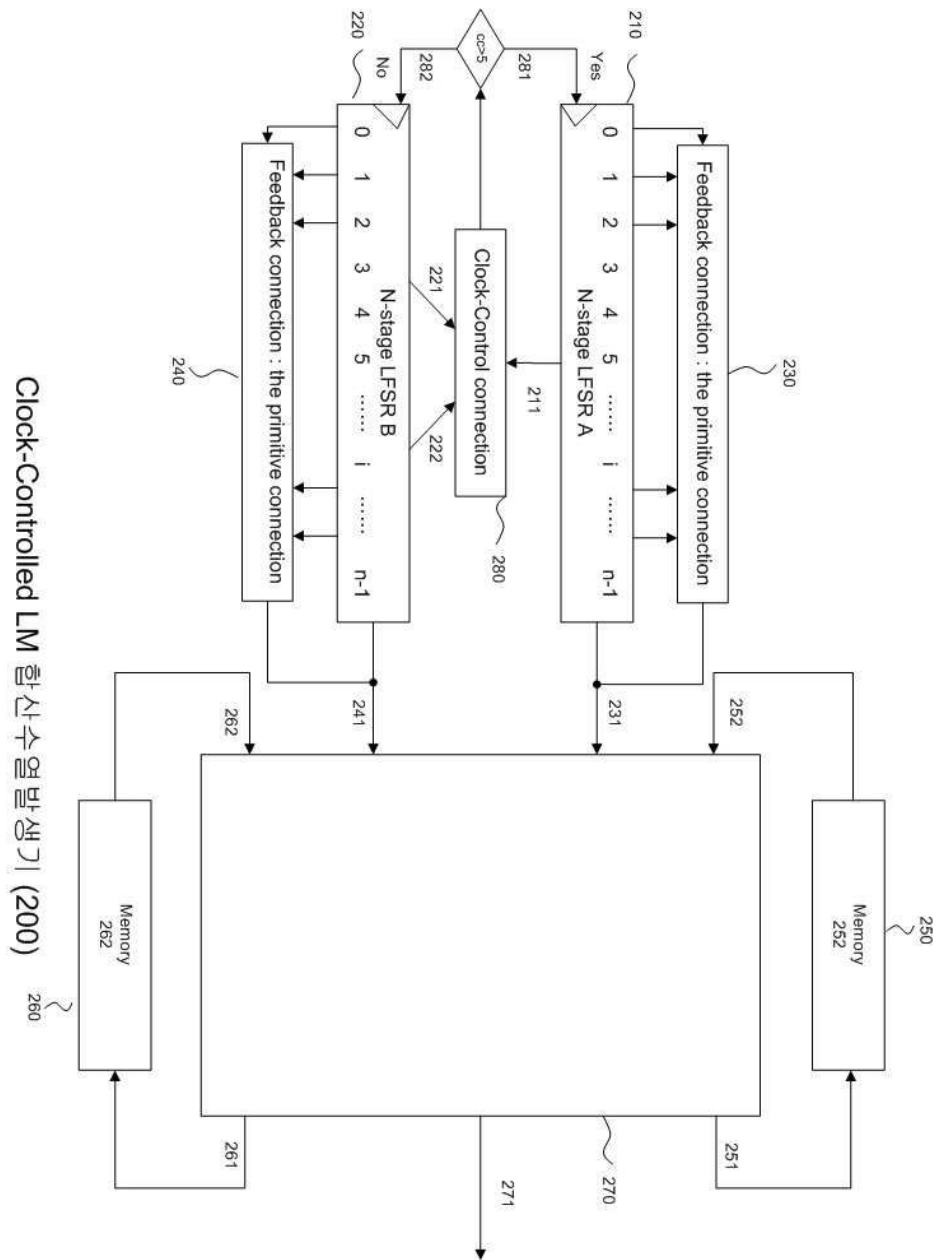
- <1> 도 1은 종래 기술에 따른 선형피드백 시프트레지스터를 사용하여 랜덤 키스트림을 생성하는 방법의 블록 구성도.
- <2> 도 2는 본 발명의 실시예에 따른 선형피드백 시프트레지스터(LFSR)의 클럭 조절을 사용하여 랜덤 키스트림을 생성하는 방법의 블록 구성도.
- <3> 도 3은 본 발명의 실시예에 따른 선형피드백 시프트레지스터(LFSR)의 클럭을 조절하는 방법의 블록 구성도

도면

도면1



도면2



Clock-Controlled LM 합산수열발생기 (200)

도면3

클럭 콘트롤 부분 (300)

