



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2019-0052226
(43) 공개일자 2019년05월16일

(51) 국제특허분류(Int. Cl.)

G06F 7/58 (2006.01)

(52) CPC특허분류

G06F 7/584 (2013.01)

(21) 출원번호 10-2017-0147725

(22) 출원일자 2017년11월08일

심사청구일자 2017년11월08일

(71) 출원인

동서대학교 산학협력단

부산광역시 사상구 주례로 47(주례동,
동서대학교)

(72) 발명자

이훈재

대구광역시 수성구 청호로85안길 11 선빌라 501호

최윤정

대구광역시 수성구 청호로 451

(뒷면에 계속)

(74) 대리인

김석계

전체 청구항 수 : 총 3 항

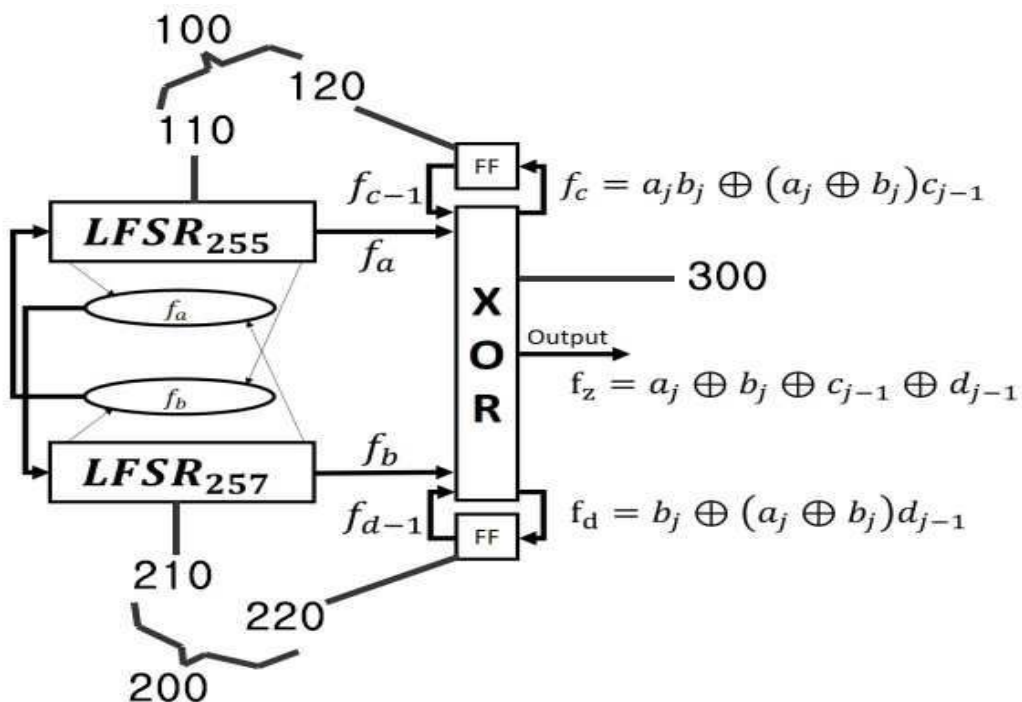
(54) 발명의 명칭 양방향성 상호 클럭조절방식을 이용한 랜덤 이진수열 발생방법

(57) 요약

본 발명 양방향성 상호 클럭조절방식을 이용한 랜덤 이진수열 발생방법은 2개의 LFSR(100, 200)이 서로 상호작용하면서 클럭을 랜덤(Random)으로 조절하여 데이터를 획득하는 데이터획득단계; 획득한 데이터를 논리회로부(300)에서 이진수열로 변환하여 발생시킨 후 최종 출력결과 z_j 를 획득하는 출력결과획득단계; 로 이루어지는 것으로

(뒷면에 계속)

대표도 - 도1



로,

본 발명은 2개의 LFSR의 메모리에 저장되는 초기값을 모두 0이 아닌 임의의 값으로 변경한 후, 각각의 LFSR의 1비트를 저장하는 캐쉬메모리를 사용하여 상호클럭조정 함수를 구성하되, LFSR의 탭 길이가 가변클럭의 횟수에 영향을 주게 되고, 상기 가변클럭의 횟수의 변화에 의해 선형복잡도가 증가하며 주기가 길어지는 것으로, 암호화된 긴 메시지를 사용하여 전달할 때, Berlekamp-Massey 알고리즘을 이용한 공격 등의 컴퓨터 공격에 대해서 안전하게 하는 현저한 효과가 있다.

(72) 발명자

김기환

부산광역시 북구 화명대로 87 현대아파트 101동
1501호

이상곤

부산광역시 서구 대영로45번길 53 보현빌리지 803
호

이 발명을 지원한 국가연구개발사업

과제고유번호 2017EG0490101

부처명 교육부

연구관리전문기관 한국연구재단

연구사업명 사회맞춤형 산학협력 선도대학(LINC+) 육성사업

연구과제명 동서대학교 사회맞춤형 산학협력 선도대학(LINC+) 육성사업(산학협력 고도화형)

기 여 율 1/2

주관기관 동서대학교 산학협력단

연구기간 2017.04.01 ~ 2022.02.28

이 발명을 지원한 국가연구개발사업

과제고유번호 2016R1D1A1B01011908

부처명 교육부

연구관리전문기관 한국연구재단

연구사업명 기본연구지원사업

연구과제명 사물인터넷/무인비행기(IoT/Drone)에 적합한 초경량-고속 암호/인증 및 물리적 해킹 방어

기술 개발

기 여 율 1/2

주관기관 동서대학교 산학협력단

연구기간 2016.06.01 ~ 2022.05.31

명세서

청구범위

청구항 1

2개의 LFSR(100, 200)이 서로 상호작용하면서 클럭을 랜덤(Random)으로 조절하여 데이터를 획득하는 데이터 획득 단계; 획득한 데이터를 논리회로부(300)에서 이진수열로 변환하여 발생시킨 후 최종 출력결과 Z_i 를 획득하는 출력결과 획득단계; 로 이루어지는 것을 특징으로 하는 양방향성 상호 클럭조절방식을 이용한 랜덤 이진수열 발생방법

청구항 2

제 1항에 있어서, 상기 2개의 LFSR(100, 200)는 제1LFSR(100)과 제2LFSR(200)로 구분되되, 각각은 메인 메모리 (110, 210)와, 1비트(bit)의 공간을 가지며 이전에 저장된 데이터를 담아두는 캐쉬 메모리(120, 220)로 이루어 지되, 상기 제1LFSR(100)과 제2LFSR(200)은 서로 다른 비트(bit)의 메인 메모리를 가지는 것을 특징으로 하는 양방향성 상호 클럭조절방식을 이용한 랜덤 이진수열 발생방법

청구항 3

제 2항에 있어서, 상기 데이터 획득단계는 제1LFSR(100)에 공급되는 클럭의 수와 제2LFSR(200)에서 생성된 이진 수열인 비선형 함수로부터 클럭 조절 함수 f_a 를 획득하며, 제2LFSR(200)에 공급되는 클럭의 수와 제 1LFSR(100)에서 생성된 이진수열인 비선형 함수로부터 클럭 조절 함수 f_b 를 획득하는 것을 특징으로 하는 양 방향성 상호 클럭조절방식을 이용한 랜덤 이진수열 발생방법

발명의 설명

기술 분야

[0001] 본 발명 양방향성 상호 클럭조절방식을 이용한 랜덤 이진수열 발생방법에 관한 것으로, 더욱 상세하게는 2개의 LFSR의 메모리에 저장되는 초기값을 모두 0이 아닌 임의의 값으로 변경한 후, 각각의 LFSR의 1비트를 저장하는 캐쉬메모리를 사용하여 상호클럭조절 함수를 구성하되, LFSR의 탭 길이가 가변클럭의 횟수에 영향을 주게 되고, 상기 가변클럭의 횟수의 변화에 의해 선형복잡도가 증가하며 주기가 길어지는 것으로, 암호화된 긴 메시지를 사 용하여 전달할 때, Berlekamp-Massey 알고리즘을 이용한 공격 등의 컴퓨터 공격에 대해서 안전하게 하는 양방향 성 상호 클럭조절방식을 이용한 랜덤 이진수열 발생방법에 관한 것이다.

배경 기술

[0003] 종래기술로서 공개특허공보 공개번호 제10-2015-0116711호의 상호보완 이진 수열을 이용한 영상 디블러링 방법 에는, 상호보완 이진 수열 집합을 이용하여 서로 다른 코드화 노출 패턴을 생성하는 단계, 상기 서로 다른 코드 화 노출 패턴을 가지도록 연속된 복수의 영상을 촬영하는 단계, 그리고 상기 연속된 복수의 영상을 디블러링하 는 단계를 포함하는 영상 디블러링 방법이라고 기재되어 있다.

[0004] 다른 종래기술로서 공개특허공보 공개번호 제10-1997-012115호의 마스크 제어 이진 수열 발생기에는, 외부의 클 력에 의해 쉬프트된 비트를 출력하는 제1 선형 레환 쉬프트 레지스터 수단과, 상기 제1 선형 레환 쉬프트 레지 스텐터 수단의 출력 중 일부 또는 전부를 입력으로 받아 마스크링 벡터를 생성하는 마스크링 벡터 생성 수단과, 상기 외부의 클럭에 의해 쉬프트된 이진 수열을 생성하는 제2 선형 레환 쉬프트 레지스터 수단, 및 상기 마스크링 벡터 생성수단으로 부터 입력되는 마스크링 벡터에 의해 상기 제2 선형 레환 쉬프트 레지스터 수단의 출력을 마스크하 는 마스크 회로 수단을 구비하는 것을 특징으로 하는 마스크 제어 이진 수열 발생기라고 기재되어 있다.

[0005] 그러나 상기와 같은 종래의 기술은 양방향성 상호 클럭조절방식을 제공하지 못하여 가변클럭을 제공하지

못하며, 선형복잡도가 낮고, 주기가 짧아서 컴퓨터 공격에 대한 안정성이 낮은 단점이 있었다.

발명의 내용

해결하려는 과제

[0007] 따라서 본 발명 양방향성 상호 클럭조절방식을 이용한 랜덤 이진수열 발생방법을 통하여, 2개의 LFSR의 메모리에 저장되는 초기값을 모두 0이 아닌 임의의 값으로 변경한 후, 각각의 LFSR의 1비트를 저장하는 캐쉬메모리를 사용하여 상호클럭조절 함수를 구성하되, LFSR의 탭 길이가 가변클럭의 횟수에 영향을 주게 되고, 상기 가변클럭의 횟수의 변화에 의해 선형복잡도가 증가하며 주기가 길어지는 것으로, 암호화된 긴 메시지를 사용하여 전달할 때, Berlekamp-Massey 알고리즘을 이용한 공격 등의 컴퓨터 공격에 대해서 안전하게 하는 양방향성 상호 클럭조절방식을 이용한 랜덤 이진수열 발생방법을 제공하고자 하는 것이다.

과제의 해결 수단

[0009] 본 발명 양방향성 상호 클럭조절방식을 이용한 랜덤 이진수열 발생방법은 2개의 LFSR(100, 200)이 서로 상호작용하면서 클럭을 랜덤(Random)으로 조절하여 데이터를 획득하는 데이터획득단계; 획득한 데이터를 논리회로부(300)에서 이진수열로 변환하여 발생시킨 후 최종 출력결과 Z_j 를 획득하는 출력결과획득단계; 로 이루어지는 것을 특징으로 한다.

발명의 효과

[0011] 본 발명은 2개의 LFSR의 메모리에 저장되는 초기값을 모두 0이 아닌 임의의 값으로 변경한 후, 각각의 LFSR의 1비트를 저장하는 캐쉬메모리를 사용하여 상호클럭조절 함수를 구성하되, LFSR의 탭 길이가 가변클럭의 횟수에 영향을 주게 되고, 상기 가변클럭의 횟수의 변화에 의해 선형복잡도가 증가하며 주기가 길어지는 것으로, 암호화된 긴 메시지를 사용하여 전달할 때, Berlekamp-Massey 알고리즘을 이용한 공격 등의 컴퓨터 공격에 대해서 안전하게 하는 현저한 효과가 있다.

도면의 간단한 설명

[0013] 도 1은 본 발명의 개념도

발명을 실시하기 위한 구체적인 내용

[0014] 본 발명 양방향성 상호 클럭조절방식을 이용한 랜덤 이진수열 발생방법은 2개의 LFSR(100, 200)이 서로 상호작용하면서 클럭을 랜덤(Random)으로 조절하여 데이터를 획득하는 데이터획득단계; 획득한 데이터를 논리회로부(300)에서 이진수열로 변환하여 발생시킨 후 최종 출력결과 Z_j 를 획득하는 출력결과획득단계; 로 이루어지는 것을 특징으로 한다.

[0015] 또한, 상기 2개의 LFSR(100, 200)는 제1LFSR(100)과 제2LFSR(200)로 구분되되, 각각은 메인 메모리(110, 210)와, 1비트(bit)의 공간을 가지며 이전에 저장된 데이터를 담아두는 캐쉬 메모리(120, 220)로 이루어지되, 상기 제1LFSR(100)과 제2LFSR(200)은 서로 다른 비트(bit)의 메인 메모리를 가지는 것을 특징으로 한다.

[0016] 또한, 상기 데이터획득단계는 제1LFSR(100)에 공급되는 클럭의 수와 제2LFSR(200)에서 생성된 이진수열인 비선형 함수로부터 클럭 조절 함수 f_a 를 획득하며, 제2LFSR(200)에 공급되는 클럭의 수와 제1LFSR(100)에서 생성된 이진수열인 비선형 함수로부터 클럭 조절 함수 f_b 를 획득하는 것을 특징으로 한다.

[0017] 또한, 상기 출력결과획득단계는 클럭 조절 함수 f_a 를 통해 계산된 a_j 와, 상기 클럭 조절 함수 f_b 를 통해

계산된 b_j 를 논리회로부(300)에 각각 입력되면, 상기 논리회로부(300)는 함수를 이용한 연산을 통해 최종 출력 결과 z_j 를 획득하는 것을 특징으로 한다.

[0018] 또한, 상기 논리회로부(300)에는 함수가 적용되고, 상기 함수는 비선형 함수인 것으로, 클럭 조절 함수 f_a 와 f_b , 캐리함수 f_c , 메모리함수 f_d , 결합함수 f_z 를 포함하는 것을 특징으로 한다.

[0020] 본 발명을 첨부 도면에 의해 상세히 설명하면 다음과 같다.

[0021] 도 1은 본 발명의 개념도이다.

[0022] 본 발명에 대해 구체적으로 기술하면, 본 발명 양방향성 상호 클럭조절방식을 이용한 랜덤 이진수열 발생방법은 2개의 LFSR(100, 200)이 서로 상호작용하면서 클럭을 랜덤(Random)으로 조절하여 데이터를 획득하는 데이터획득 단계; 획득한 데이터를 논리회로부(300)에서 이진수열로 변환하여 발생시킨 후 최종 출력결과 z_j 를 획득하는 출력결과획득단계; 로 이루어지는 것이다.

[0023] 특히, 상기 2개의 LFSR(100, 200)는 제1LFSR(100)과 제2LFSR(200)로 구분되되, 각각은 메인 메모리(110, 210)와, 1비트(bit)의 공간을 가지며 이전에 저장된 데이터를 담아두는 캐쉬 메모리(120, 220)로 이루어지고, 제1LFSR(100)은 255비트(bit)의 메인 메모리(110)를 가지며, 제2LFSR(200)은 257비트(bit)의 메인 메모리(210)를 가지는 것이다.

[0024] 상기 제1LFSR(100)은 255비트(bit)이므로 내부에 연산되는 다항식은 $LFSR_{255}$ 로 표현하며, 상기 제2LFSR(200)은 257비트(bit)이므로 내부에 연산되는 다항식은 $LFSR_{257}$ 로 표현한다.

[0025] 상기 제1LFSR(100)의 다항식의 실시예는 식 1과 같다.

$$LFSR_{255} = x^{255} + x^{254} + x^{253} + x^{248} + x^{247} + x^{245} + x^{244} + \dots + x^6 + x^5 + x^4 + 1$$

(식 1)

[0027] 상기 제2LFSR(200)의 다항식의 실시예는 식 2와 같다.

$$LFSR_{257} = x^{257} + x^{250} + x^{248} + x^{246} + x^{244} + x^{242} + x^{238} + \dots + x^8 + x^3 + x^2 + x + 1$$

(식 2)

[0031] 한편, 상기 논리회로부(300)에는 함수가 적용되고, 상기 함수는 비선형 함수인 것으로, 클럭 조절 함수 f_a 와 f_b , 캐리함수 f_c , 메모리함수 f_d , 결합함수 f_z 를 포함한다.

[0032] 더욱 상세하게는, 상기 클럭 조절 함수 f_a 와 f_b 는 2개의 LFSR(100, 200)의 클럭을 제어하는 함수이며, 상기 캐리함수 f_c 는 $f_c = a_j b_j + (a_j + b_j) * c_{j-1}$ 이며, 상기 메모리함수 f_d 는 $f_d = b_j + (a_j + b_j) * d_{j-1}$ 이며, 상기 결합함수 f_z 는 $f_z = a_j + b_j + c_{j-1} + d_{j-1}$ 인 것이며, 상기 캐리함수 f_c 를 통해 캐리상태 c_j 가 결정되며, 상기 메모리함수 f_d 를 통해 메모리상태 d_j 가 결정되며, 상기 결합함수 f_z 를 통해 최종 출력결과 z_j 가 결정된다.

[0033] 도 1에 도시된 바와 같이, a_j 는 255bit인 제1LFSR(100)의 출력결과이며, b_j 는 257bit인 제2LFSR(200)의 출력

결과이며, c_j 는 캐리상태이며, c_{j-1} 는 이전 캐리상태이며, d_j 는 메모리상태이며, d_{j-1} 는 이전 메모리상태이며, z_j 는 최종 출력결과이다.

[0035] 한편, 상기 데이터획득단계는 제1LFSR(100)에 공급되는 클럭의 수와 제2LFSR(200)에서 생성된 이진수열인 비선형 함수로부터 클럭 조절 함수 f_a 를 획득하며, 제2LFSR(200)에 공급되는 클럭의 수와 제1LFSR(100)에서 생성된 이진수열인 비선형 함수로부터 클럭 조절 함수 f_b 를 획득한다.

[0036] 이때, 상기 데이터획득단계에서는 클럭 조절 함수 f_a 와 f_b 로 임의의 2개의 비트를 사용하여 가변클럭을 적용하고, 임의의 2개의 비트를 통해 계산하는 것으로, 실시에는 식 3,4와 같다.

[0037] (식 3)
$$f_a = 2 * LFSR_1[83] + LFSR_1[193] + 1$$

[0038] (식 4)
$$f_b = 2 * LFSR_2[85] + LFSR_2[197] + 1$$

[0039] 상기 가변클럭이 적용된 클럭 조절 함수 f_a 와 f_b 를 사용하여 획득한 데이터를 통해 랜덤성을 향상시켰다.

[0041] 그리고 상기 최종결과획득단계는 클럭 조절 함수 f_a 를 통해 계산된 a_j 와, 상기 클럭 조절 함수 f_b 를 통해 계산된 b_j 를 논리회로부(300)에 각각 입력되면, 상기 논리회로부(300)는 함수를 이용한 연산을 통해 최종 출력결과 z_j 를 획득하는 것이다.

[0042] 더욱 상세하게는, 상기 논리회로부(300)는 a_j 와 b_j 를 통해 캐리함수 f_c 와 메모리함수 f_d 를 연산하는 것으로, 캐리함수 f_c 를 연산하여 제1LFSR(100)의 캐시 메모리(120)에 저장하며, 상기 메모리함수 f_d 를 연산하여 제2LFSR(200)의 캐시 메모리(220)에 저장되되, 제1LFSR(100)의 캐시 메모리(120)에 저장되어있던 이전 캐리상태 c_{j-1} 와, 제2LFSR(200)의 캐시 메모리(220)에 저장되어 있던 이전 메모리상태 d_{j-1} 를 불러오며, 상기 이전 캐리상태 c_{j-1} 와, 이전 메모리상태 d_{j-1} 를 통해 결합함수 f_z 를 연산하여 랜덤(Random) 이진수열인 최종 출력결과 z_j 를 획득하는 것이다.

[0045] 한편, 상기 최종 출력결과 z_j 를 얻기 위해서는, 각각의 LFSR(100, 200)가 정해진 길이만큼 메인 메모리(110, 210)에 데이터를 저장시, 다항식의 각각의 항의 초기값이 아닌 임의의 값으로 연산되어 저장되며, 주기는 $2^n - 1$ 이 된다.

[0046] 이때, 상기 최종 출력결과 z_j 는 스트림 암호인 것으로, 랜덤(Random)한 난수를 연속적으로 생성하여 데이터와 결합됨으로써 암호화 된 것이다.

- [0049] 상기 2개의 LFSR(100, 200)는 초기에 초기화를 위한 초기화 단계를 실시한다.
- [0050] 상기 초기화 단계에서 키(key)와 초기화 벡터(IV, Initialization Vector)로부터 내부상태가 채워지되, 각 데이터는 '0'이 아닌 임의의 값으로 채우고, 캐리함수와 메모리함수를 초기화한다. 이후 각각의 LFSR(100, 200)에서 임의의 2개 비트를 사용하여 상호클럭조절 함수를 적용하는 것이다.
- [0051] 특히, 상기 내부상태의 길이가 키(key) 길이보다 더 길기 때문에, 키 확장을 하여 내부상태를 채운다.
- [0052] 그리고 상기 2개의 LFSR(100, 200)의 길이가 가변클럭의 횟수에 영향을 미치며, 제1LFSR(100)의 짧은 탭에 관한 원시다항식과 제2LFSR(200)의 긴 탭에 관한 원시다항식은 모두 최대 주기를 보장하지만 상대적으로 제2LFSR(200)의 긴 탭에 관한 원시다항식이 보다 복잡한 상태값을 가지게 된다.
- [0053] 이를 해결하는 첫 번째 방법은, 가변클럭의 횟수를 임의의 지정된 횟수로 지정하여 사용하는 것이며, 두 번째 방법은, 각각의 LFSR(100, 200)의 원시다항식을 변경하여 출력 순서를 변경하는 것으로, 안전성을 향상시킬 수 있다.
- [0055] 특히, 상기 최종 출력결과 Z_j , 즉 스트림 암호의 안전성을 확인하는 기본 요구사항은 주기 및 선형복잡도이며, 특히, 주기가 길수록, 선형복잡도가 높을 수록, Berlekamp-Massey 알고리즘 등을 이용한 컴퓨터 공격에 견디기 쉽다.
- [0056] 특히, 본 발명에서 제1LFSR(100)은 255비트, 제2LFSR(200)은 257비트를 사용하고 있으므로, 최대주기는 약 $2^{512}-1$ 이 되나, 상호클럭조절 함수가 임의적으로 최대 4비트의 클럭을 동작시킬 수 있으므로, 주기는 P로 표현하되, 약 $2^{508}-1 \leq P \leq 2^{512}-1$ 로 계산하는 것이며, 선형복잡도의 경우에도 LM 합성수열의 특성에 따라 주기와 유사한 결과를 나타내며, 설계 기준강도가 2^{256} 이므로, 컴퓨터 공격에 대하여 안전할 수 있다.
- [0057] 예를들면, 컴퓨터 공격을 하는 사용자가 슈퍼 컴퓨터를 사용할 시, 슈퍼 컴퓨터의 연산 능력이 1초에 약 2^{50} 인 부분을 감안하면, 최소 연산시간이 약 2^{458} 초이 되며, 1년을 초로 환산할 경우 약 2^{25} 로 계산되어 컴퓨터 공격을 하기 위해서는 약 2^{433} 년이 필요함을 판단할 수 있다.
- [0060] 따라서 본 발명은 2개의 LFSR의 메모리에 저장되는 초기값을 모두 0이 아닌 임의의 값으로 변경한 후, 각각의 LFSR의 1비트를 저장하는 캐시메모리를 사용하여 상호클럭조절 함수를 구성하되, LFSR의 탭 길이가 가변클럭의 횟수에 영향을 주게 되고, 상기 가변클럭의 횟수의 변화에 의해 선형복잡도가 증가하며 주기가 길어지는 것으로, 암호화된 긴 메시지를 사용하여 전달할 때, Berlekamp-Massey 알고리즘을 이용한 공격 등의 컴퓨터 공격에 대해서 안전하게 하는 현저한 효과가 있다.

부호의 설명

- [0061] 100 : 제1LFSR
- 200 : 제2LFSR
- 110, 210 : 메인 메모리
- 120, 220 : 캐시 메모리
- 300 : 논리회로부

도면

도면1

