(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2011년01월21일
(11) 등록번호 10-1010226
(24) 등록일자 2011년01월17일

(51) Int. Cl.
H04L 9/32 (2006.01) *H04L 9/26* (2006.01)
H04L 12/22 (2006.01) *H04L 9/28* (2006.01)
(21) 출원번호 10-2005-7017319
(22) 출원일자(국제출원일자) 2003년03월25일
심사청구일자 2008년02월26일
(85) 번역문제출일자 2005년09월15일
(65) 공개번호 10-2005-0119121
(43) 공개일자 2005년12월20일
(86) 국제출원번호 PCT/JP2003/003595
(87) 국제공개번호 WO 2004/086673
국제공개일자 2004년10월07일
(56) 선행기술조사문헌
Marco Tomassini and Mathieu Perrenoud, "Cryptography with cellular automata," Applied Soft Computing, Volume 1, Issue 2, Pages 151-160
US20030076956 A1
US20040141614 A1
US20030204541 A1
전체 청구항 수 : 총 18 항

(73) 특허권자
도꾸리츠 교세이 호징 죠우호 쯔우신 겐큐 기코우
일본국 도쿄도 코가네이시 누쿠이-키타마치 4쵸메 2-1
(72) 발명자
김성주
일본국 도쿄도 코가네이시 누쿠이-키타마치 4쵸메 2-1 도꾸리츠교세이 호징 죠우호 쯔우신 겐큐 기코우내
하세가와 아키오
일본국 도쿄도 코가네이시 누쿠이-키타마치 4쵸메 2-1 도꾸리츠교세이 호징 죠우호 쯔우신 겐큐 기코우내
우메노 겐
일본국 도쿄도 코가네이시 누쿠이-키타마치 4쵸메 2-1 도꾸리츠교세이 호징 죠우호 쯔우신 겐큐 기코우내
(74) 대리인
유미특허법인

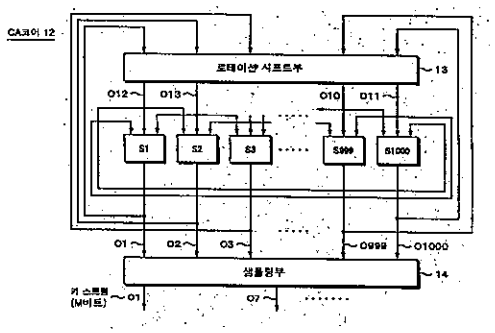
심사관 : 이형일

(54) 난수 생성, 암호화 및 복호를 위한 장치, 방법, 프로그램,및 기록 매체

(57) 요 약

본 발명은 난수 생성, 암호화 및 복호를 위한 장치, 방법, 프로그램, 및 기록 매체에 관한 것으로서, 암호화를 위한 난수(亂數)가 CA코어에 의해 생성된다. CA코어는, 1차원 2상태 3근방 셀 오토맨(cell automan)의 구성으로 된다. 셀의 각 셀에 대하여는, 자체와 양 옆의 셀에 대한 합계 3개의 입력이 공급된다. 각 셀은, 논리 연산을 행하고, 논리 연산 결과를 출력한다. 각 셀에는, 레지스터가 포함되고, 각 레지스터가 클록에 동기하여 논리 연산 결과를 차례로 취하여, 유지한다. 셀의 출력이 다음의 타임 스텝의 연산을 위해, 셀에 대하여 피드백되지만, 그 경우에, 출력을 좌측으로 시프트시켜 셀에 피드백하는 로테이션 시프트 조작이 행해진다. 다수개의 난수로서 출력하기 위해, 셀의 출력 중 40비트가 선택된다. 선택되는 셀 번호는, 등 간격이 아니고, 선택되는 셀 번호의 간격이 서서히 커지게 된다.

대 표 도 - 도9



특허청구의 범위

청구항 1

1차원적으로 복수개의 셀이 배치되고, 각 셀이 상태값으로서 0이나 1을 가지고, 다음 시각에서의 각 셀의 상태값은 자체의 상태값과 근방의 셀 상태값에만 의존하는 룰에 의해 주어지고, 각 셀의 상태값은 상기 룰에 의해 갱신되는 1차원 2상태 K근방 셀 오토맨(cell automan)에 의한 난수(亂數) 생성 장치에 있어서,

복수개의 셀의 출력을 샘플링 수단에 입력하고, 상기 복수개의 셀의 다음 시각의 상태값을 갱신하기 위해, 현재 시각의 상기 복수개의 셀의 출력을 입력으로 피드백하는 경로와,

상기 경로에 삽입되고, 상기 복수개의 셀의 출력을 2 이상의 소정의 셀수만큼 시프트하는 시프트 처리 수단과,

상기 복수개의 셀의 출력 중, 소정의 복수개의 셀을 선택하여 병렬화하여 출력하기 위한 상기 샘플링 수단

을 구비하고,

상기 소정의 복수개의 셀은 선택되는 셀의 서로의 간격이 순차적으로 커지거나 또는 순차적으로 작아지는,

난수 생성 장치.

청구항 2

제1항에 있어서,

상기 1차원 2상태 K근방 셀 오토맨은, 다음 시각에서의 각 셀의 상태값은 자체의 상태값과 양 옆의 셀 상태값에만 의존하는 룰에 의해 주어지고, 각 셀의 상태값은 상기 룰에 의해 갱신되는 1차원 2상태 3근방 셀 오토맨인 것을 특징으로 하는 난수 생성 장치.

청구항 3

삭제

청구항 4

삭제

청구항 5

제1항에 있어서,

상기 피드백하는 경로 및 상기 시프트 처리 수단이 집적 회로 상에 실현된 것을 특징으로 하는 난수 생성 장치.

청구항 6

복수개의 셀의 각 셀이 상태값으로서 0이나 1을 가지고, 다음 시각에서의 각 셀의 상태값은 자체의 상태값과 근방의 셀 상태값에만 의존하는 룰에 의해 주어지고, 각 셀의 상태값은 상기 룰에 의해 갱신되는 1차원 2상태 K근방 셀 오토맨에 의한 난수 생성 방법에 있어서,

복수개의 셀의 출력을 샘플링 수단으로 출력하고, 상기 복수개의 셀의 다음 시각의 상태값을 갱신하기 위해, 현재 시각의 상기 복수개의 셀의 출력을 입력으로 피드백할 때, 상기 복수개의 셀의 출력을 2 이상의 소정의 셀수만큼 시프트하고,

상기 샘플링 수단이 상기 복수개의 셀의 출력 중 소정의 복수개의 셀을 선택하여 병렬화하여 출력하고, 상기 소정의 복수개의 셀은 선택되는 셀의 서로의 간격이 순차적으로 커지거나 또는 순차적으로 작아지는,

난수 생성 방법.

청구항 7

제6항에 있어서,

상기 1차원 2상태 K근방 셀 오토맨은, 다음 시각에서의 각 셀의 상태값은 자체의 상태값과 양 옆의 셀 상태값

에만 의존하는 룰에 의해 주어지고, 각 셀의 상태값은 상기 룰에 의해 갱신되는 1차원 2상태 3근방 셀 오토맨인 것을 특징으로 하는 난수 생성 방법.

청구항 8

삭제

청구항 9

삭제

청구항 10

삭제

청구항 11

컴퓨터에 대하여, 복수개의 셀의 각 셀이 상태값으로서 0이나 1을 가지고, 다음 시각에서의 각 셀의 상태값은 자체의 상태값과 근방의 셀 상태값에만 의존하는 룰에 의해 주어지고, 각 셀의 상태값은 상기 룰에 의해 갱신되는 1차원 2상태 K근방 셀 오토맨에 의한 난수 생성 방법을 실행하도록 하기 위한 프로그램이 기록된, 컴퓨터로 판독 가능한 기록 매체에 있어서,

복수개의 셀의 출력을 샘플링 수단으로 출력하고, 상기 복수개의 셀의 다음 시각의 상태값을 갱신하기 위해, 현재 시각의 상기 복수개의 셀의 출력을 입력으로 피드백할 때, 상기 복수개의 셀의 출력을 2 이상의 소정의 셀수만큼 시프트하고,

상기 샘플링 수단은 상기 복수개의 셀의 출력 중 소정의 복수개의 셀을 선택하여 병렬화하여 출력하고, 상기 소정의 복수개의 셀은 선택되는 셀의 서로의 간격이 순차적으로 커지거나 또는 순차적으로 작아지는,

난수 생성 방법을 실행하도록 하기 위한 프로그램이 기록된, 컴퓨터로 판독 가능한 기록 매체.

청구항 12

평문(平文)과 난수의 배타적 논리합에 의해 암호문을 생성하는 암호화 장치에 있어서,

상기 난수는, 1차원적으로 복수개의 셀이 배치되고, 각 셀이 상태값으로서 0이나 1을 가지고, 다음 시각에서의 각 셀의 상태값은 자체의 상태값과 근방의 셀 상태값에만 의존하는 룰에 의해 주어지고, 상기 각 셀의 상태값은 상기 룰에 의해 갱신되는 1차원 2상태 K근방 셀 오토맨에 의한 난수 생성 장치에 의해 생성되고,

복수개의 셀의 출력을 샘플링 수단에 출력하고, 상기 복수개의 셀의 다음 시각의 상태값을 갱신하기 위해, 현재 시각의 상기 복수개의 셀의 출력을 입력으로 피드백하는 경로와,

상기 경로에 삽입되고, 상기 복수개의 셀의 출력을 2 이상의 소정의 셀수만큼 시프트하는 시프트 처리 수단과,

상기 복수개의 셀의 출력 중, 소정의 복수개의 셀을 선택하여 병렬화하여 출력하기 위한 상기 샘플링 수단

을 구비하고,

상기 소정의 복수개의 셀은 선택되는 셀의 서로의 간격이 순차적으로 커지거나 또는 순차적으로 작아지는,

암호화 장치.

청구항 13

제12항에 있어서,

상기 1차원 2상태 K근방 셀 오토맨은, 다음 시각에서의 각 셀의 상태값은 자체의 상태값과 양 옆의 셀 상태값에만 의존하는 룰에 의해 주어지고, 각 셀의 상태값은 상기 룰에 의해 갱신되는 1차원 2상태 3근방 셀 오토맨인 것을 특징으로 하는 암호화 장치.

청구항 14

삭제

청구항 15

삭제

청구항 16

제13항에 있어서,

상기 피드백하는 경로 및 상기 시프트 처리 수단이 집적 회로 상에 실현된 것을 특징으로 하는 암호화 장치.

청구항 17

평문과 난수의 배타적 논리합에 의해 암호문을 생성하는 암호화 방법에 있어서,

상기 난수는, 복수개의 셀의 각 셀이 상태값으로서 0이나 1을 가지고, 다음 시각에서의 각 셀의 상태값은 자체의 상태값과 근방의 셀 상태값에만 의존하는 룰에 의해 주어지고, 각 셀의 상태값은 상기 룰에 의해 갱신되는 1차원 2상태 K근방 셀 오토맨에 의한 난수 생성 방법에 의해 생성되고,

상기 난수 생성 방법은, 복수개의 셀의 출력을 샘플링 수단에 출력하고, 상기 복수개의 셀의 다음 시각의 상태값을 갱신하기 위해, 현재 시각의 상기 복수개의 셀의 출력을 입력으로 피드백하고, 피드백할 때 상기 복수개의 셀의 출력을 2 이상의 소정의 셀수만큼 시프트하며,

상기 난수 생성 방법은, 상기 샘플링 수단에서 상기 복수개의 셀의 출력 중 소정의 복수개의 셀을 선택하여 병렬화하여 출력하고, 상기 소정의 복수개의 셀은 선택되는 셀의 서로의 간격이 순차적으로 커지거나 또는 순차적으로 작아지는,

암호화 방법.

청구항 18

제17항에 있어서,

상기 1차원 2상태 K근방 셀 오토맨은, 다음 시각에서의 각 셀의 상태값은 자체의 상태값과 양 옆의 셀 상태값에만 의존하는 룰에 의해 주어지고, 각 셀의 상태값은 상기 룰에 의해 갱신되는 1차원 2상태 3근방 셀 오토맨인 것을 특징으로 하는 암호화 방법.

청구항 19

삭제

청구항 20

삭제

청구항 21

삭제

청구항 22

컴퓨터에 대하여, 평문과 난수의 배타적 논리합에 의해 암호문을 생성하는 암호화 방법을 실행하도록 하기 위한 프로그램이 기록된, 컴퓨터로 판독 가능한 기록 매체에 있어서,

상기 난수는, 복수개의 셀의 각 셀이 상태값으로서 0이나 1을 가지고, 다음 시각에서의 각 셀의 상태값은 자체의 상태값과 근방의 셀 상태값에만 의존하는 룰에 의해 주어지고, 각 셀의 상태값은 상기 룰에 의해 갱신되는 1차원 2상태 K근방 셀 오토맨에 의한 난수 생성 방법에 의해 생성되고,

상기 난수 생성 방법은, 복수개의 셀의 출력을 샘플링 수단에 출력하고, 상기 복수개의 셀의 다음 시각의 상태값을 갱신하기 위해, 현재 시각의 상기 복수개의 셀의 출력을 입력으로 피드백할 때, 상기 복수개의 셀의 출력을 2 이상의 소정의 셀수만큼 시프트하고,

상기 난수 생성 방법은, 상기 샘플링 수단에서 상기 복수개의 셀의 출력 중 소정의 복수개의 셀을 선택하여 병

렬화하여 출력하고, 상기 소정의 복수개의 셀은 선택되는 셀의 서로의 간격이 순차적으로 커지거나 또는 순차적으로 작아지는,

암호화 방법을 실행하도록 하기 위한 프로그램이 기록된, 컴퓨터로 판독 가능한 기록 매체.

청구항 23

암호문과 난수의 배타적 논리합에 의해 암호문을 복호하는 복호 장치에 있어서,

상기 난수는, 1차원적으로 복수개의 셀이 배치되고, 각 셀이 상태값으로서 0이나 1을 가지고, 다음 시각에서의 각 셀의 상태값은 자체의 상태값과 근방의 셀 상태값에만 의존하는 룰에 의해 주어지고, 각 셀의 상태값은 상기 룰에 의해 갱신되는 1차원 2상태 K근방 셀 오토맨에 의한 난수 생성 장치에 의해 생성되고,

복수개의 셀의 출력을 샘플링 수단에 출력하고, 상기 복수개의 셀의 다음 시각의 상태값을 갱신하기 위해, 현재 시각의 상기 복수개의 셀의 출력을 입력으로 피드백하는 경로와,

상기 경로에 삽입되고, 상기 복수개의 셀의 출력을 2 이상의 소정의 셀수만큼 시프트하는 시프트 처리 수단과,

상기 복수개의 셀의 출력 중, 소정의 복수개의 셀을 선택하여 병렬화하여 출력하기 위한 상기 샘플링 수단

을 구비하고,

상기 소정의 복수개의 셀은 선택되는 셀의 서로의 간격이 순차적으로 커지거나 또는 순차적으로 작아지는,

복호 장치.

청구항 24

제23항에 있어서,

상기 1차원 2상태 K근방 셀 오토맨은, 다음 시각에서의 각 셀의 상태값은 자체의 상태값과 양 옆의 셀 상태값에만 의존하는 룰에 의해 주어지고, 각 셀의 상태값은 상기 룰에 의해 갱신되는 1차원 2상태 3근방 셀 오토맨인 것을 특징으로 하는 복호 장치.

청구항 25

제23항에 있어서,

상기 피드백하는 경로 및 상기 시프트 처리 수단이 집적 회로 상에 실현된 것을 특징으로 하는 복호 장치.

청구항 26

암호문과 난수의 배타적 논리합에 의해 암호문을 복호하는 복호 방법에 있어서,

상기 난수는, 복수개의 셀의 각 셀이 상태값으로서 0이나 1을 가지고, 다음 시각에서의 각 셀의 상태값은 자체의 상태값과 근방의 셀 상태값에만 의존하는 룰에 의해 주어지고, 각 셀의 상태값은 상기 룰에 의해 갱신되는 1차원 2상태 K근방 셀 오토맨에 의한 난수 생성 방법에 의해 생성되고,

상기 난수 생성 방법은, 복수개의 셀의 출력을 샘플링 수단에 출력하고, 상기 복수개의 셀의 다음 시각의 상태값을 갱신하기 위해, 현재 시각의 상기 복수개의 셀의 출력을 입력으로 피드백할 때, 상기 복수개의 셀의 출력을 2 이상의 소정의 셀수만큼 시프트하고,

상기 난수 생성 방법은, 상기 샘플링 수단에서 상기 복수개의 셀의 출력 중 소정의 복수개의 셀을 선택하여 병렬화하여 출력하고, 상기 소정의 복수개의 셀은 선택되는 셀의 서로의 간격이 순차적으로 커지거나 또는 순차적으로 작아지는,

복호 방법.

청구항 27

제26항에 있어서,

상기 1차원 2상태 K근방 셀 오토맨은, 다음 시각에서의 각 셀의 상태값은 자체의 상태값과 양 옆의 셀 상태값에만 의존하는 룰에 의해 주어지고, 각 셀의 상태값은 상기 룰에 의해 갱신되는 1차원 2상태 3근방 셀 오토맨

인 것을 특징으로 하는 복호 방법.

청구항 28

삭제

청구항 29

컴퓨터에 대하여, 암호문과 난수의 배타적 논리합에 의해 암호문을 복호하는 복호 방법을 실행하도록 하기 위한 프로그램이 기록된, 컴퓨터로 판독 가능한 기록 매체에 있어서,

상기 난수는, 복수개의 셀의 각 셀이 상태값으로서 0이나 1을 가지고, 다음 시각에서의 각 셀의 상태값은 자체의 상태값과 근방의 셀 상태값에만 의존하는 룰에 의해 주어지고, 각 셀의 상태값은 상기 룰에 의해 갱신되는 1차원 2상태 K근방 셀 오토맨에 의한 난수 생성 방법에 의해 생성되고,

상기 난수 생성 방법은, 복수개의 셀의 출력을 샘플링 수단에 출력하고, 상기 복수개의 셀의 다음 시각의 상태값을 갱신하기 위해, 현재 시각의 상기 복수개의 셀의 출력을 입력으로 피드백할 때, 상기 복수개의 셀의 출력을 2 이상의 소정의 셀수만큼 시프트하고,

상기 난수 생성 방법은, 상기 샘플링 수단에서 상기 복수개의 셀의 출력 중 소정의 복수개의 셀을 선택하여 병렬화하여 출력하고, 상기 소정의 복수개의 셀은 선택되는 셀의 서로의 간격이 순차적으로 커지거나 또는 순차적으로 작아지는,

복호 방법을 실행하도록 하기 위한 프로그램이 기록된, 컴퓨터로 판독 가능한 기록 매체.

명 세 서

기 술 분 야

[0001] 본 발명은, 예를 들면 스트림 암호화에 적용되는 난수(亂數) 생성, 암호화 및 복호를 위한 장치, 방법, 프로그램, 및 기록 매체에 관한 것이다.

배 경 기 술

[0002] 최근의 인터넷이나 모바일 커뮤니케이션의 급속한 보급에 따라, 디지털 정보의 보호의 중요성이 증대하고 있다. 암호 기술로서, 암호화와 복호에 같은 비밀키를 사용하는 공통키 방식이 알려져 있고, 공통키 방식 중에, 블록 암호와 스트림 암호가 있다.

[0003] 도 1 (A)는, 블록 암호를 설명하는 것이다. 평문(平文)의 정보 비트열을 소정의 길이(블록)로 구획하고, 블록마다 암호화기(1)에 의해 암호화한다. 암호화문도 블록마다 구획되어 있다.

[0004] 한편, 도 1 (B)에 나타낸 바와 같이, 스트림 암호의 경우에는, 암호화기(난수 생성기)(2)에 의해 발생한 난수를 비트마다 정보 비트열에 대하여 작용시켜 암호화를 행한다.

[0005] 스트림 암호에 있어서는, 평문의 비트 계열을 m1, m2, m3, …로 하고, 난수의 비트 계열을 r1, r2, r3, …로 하고, 암호문의 비트 계열을 c1, c2, c3, …로 하면, 암호화 처리는, $ci = mi \oplus ri$($\oplus$는, mod.2의 연산, i= 1, 2, 3, …으로 되고, 복호 처리는, $mi = ci \oplus ri$($\oplus$는, mod.2의 연산, i= 1, 2, 3, …으로 된다.

[0006] 송신측과 수신측에서 공통의 난수를 생성하는 것이 필요해진다. 난수열 또는 난수 생성의 패턴이 알려져 버리면, 용이하게 해독되어 버린다. 따라서, 암호용으로서 안전한 난수는, 통계적인 난수의 일양성(一樣性)만아니라, 과거의 난수열로부터 장래의 난수열이 예측 불가능해야 할 필요도 있다.

[0007] 일반적으로 스트림 암호 쪽이 블록 암호보다 고속이며, 화상 데이터와 같은 대량의 데이터를 암호화하여 전송하는 경우에는, 스트림 암호 쪽이 적합하다. 또, 스트림 암호 쪽이 회로 규모를 작게 할 수 있는 경우가 많다. 그러므로, DES(Data Encryption Standard)나 AES(Advanced Encryption Standard) 등의 블록 암호가 표준화되어 있음에도 불구하고, 스트림 암호가 사용되고 있다.

[0008] 그러나, 현재 가장 널리 사용되고 있는 스트림 암호인 RC4((Rivest Cipher) 4 Stream Cipher)는, weak key의

존재, WEP(Wired Equivalent Privacy protocol)를 사용하는 것에 의한 문제점, 아웃풋에 있어서의 바이어스의 존재 등, 그 안전성이 아카데믹한 의미로 문제시되고 있다. 또, RC4는, 소프트 웨어 전용으로 디자인된 것이며, 그 암호화 속도에는 한계가 있다. 이로부터, 하드웨어 전용의 안전하며 고속의 스트림 암호가 요구되고 있다고 할 수 있다.

[0009] 한편, 비선형 역학계의 분야에서 연구되어 온 카오스를 이용한 암호화 알고리즘이 최근 활발히 연구되고 있다. 그러나, 그 대부분은, 사상(寫像) 역학계에 기초하고 있고, 시간, 공간이 모두 이산(離散)인 역학계인 셀 오토맨(cell automan; 이하, 적당히 CA라고 함)를 사용한 암호화 알고리즘은, 널리 알려져 있지 않다. CA는, 그 구성 상 하드웨어의 매립에 적합하여, 고속의 스트림 암호의 실현이 기대된다. Stephen Wolfram은, "Adv.Appl.Math.Vol.7(1986) 123-169", "Lecture Notes in Computer Science Vol.218(1986) 429-432" 등에 있어서, 1차원 2상태 3근방 셀 오토맨의 룰 30을 이용한 스트림 암호를 제안하고 있다.

[0010] 도 2는, CA를 사용한 암호화 알고리즘에 의한 구성을 나타낸다. 입력 정보 데이터(평문)가 1비트의 스트림으로서 배타적 논리합 회로(이하, 적당히 EX-OR 게이트라고 함)(3)에 입력된다. CA코어(4)(난수 생성기)로부터의 1비트의 스트림인 키스트림이 EX-OR 게이트(3)의 다른 쪽의 입력으로 되고, EX-OR 게이트(3)로부터의 암호문이 출력된다. CA코어(4)에 대하여는, 초기값으로서의 시크릿키와 클록이 입력되어, 난수가 생성된다.

[0011] 1차원 2상태 3근방 셀 오토맨이란, 1차원 격자 상에 셀이 배치되고, 각 셀은, 상태값으로서 0이나 1을 가지는 것으로 하고, 다음 시각(이하, 타임 스텝이라고 함)에서의 각 셀의 상태값은, 자체의 상태값과 양 인접하는 상태값에만 의존하는 함수(룰)로 부여되고, 각 셀의 상태값은, 이 함수에 의해 동기적으로 갱신된다. 즉, 하기의 식(1)로 표현된다.

[0012] $$S_i^{t+1} = F\left(S_{i-1}^t, S_i^t, S_{i+1}^t\right) \qquad (1)$$

[0013] 여기서, i 및 t가 부가된 S는, 타임 스텝 t에서의 i번째의 셀 상태를 나타낸다.

[0014] Stephen Wolfram는, 랜덤열을 생성하는 룰을 1차원 2상태 3근방 CA의 범위에서 탐색하고, 룰 30이 가장 양호한 의사(擬似) 난수 생성기인 것을 나타낸다. 상기 룰 30 상태 갱신 룰은,하기의 식(2)로 표현된다.

[0015] $$S_i^{t+1} = S_{i-1}^t \oplus S_i^t \oplus S_{i+1}^t \oplus S_i^t \cdot S_{i+1}^t \qquad (2)$$

[0016] 여기서, $\oplus$는, mod.2의 가산을 나타낸다.

[0017] 식(2)을 불 대수(Booleans algebra)로 나타내면, 이하의 식(3)에서 나타낸 것으로 된다.

[0018] $$S_i^{t+1} = S_{i-1}^t XOR\left(S_i^t \; OR \; S_{i+1}^t\right) \qquad (3)$$

[0019] 도 3은, 세로축에 시간(t)을 취하고, 가로축에 셀 번호(i)를 취한 도면을 나타낸다. 도 3에서는, 그림자를 부여한 i번째 예를 들면 제6 번의 셀 번호 상태가 키스트림으로서 사용되는 것을 나타내고 있다.

[0020] Stephen Wolfram은, CA를 30이 생성하는 비트열을 7종류의 통계 테스트에 걸쳐 그 랜덤성을 조사했지만, 비트열의 랜덤성을 몇개인가 조사한 것만으로는, 의사 난수 생성기로서의 성능 평가로서는 불충분한 것이었다.

[0021] 암호용의 난수로서의 평가의 시험으로 하고, 일례로서, NIST(National Institute of Standards and Technology: 미국 표준 기술 연구소)가 공개하고 있는 RNG Testing가 있다(NIST Special Publication(SP) 800-22 A Statistical Test Suite for Randomand Pseudo random Number Generators for Cryptographic Applications). 도 4는, NIST의 16종류의 테스트 항목을 나타낸다.

[0022] NIST의 테스트에서는, t비트의 열에 대하여 p-value를 구한다. p-value는, 이론상의 완전한 랜덤열 생성기가 그 비트열로부터 랜덤성이 낮은 비트열을 낼 확률이다. 여기서의 「랜덤성이 낮다」란, 테스트하고 있는 특성량이 평균값으로부터 벌어지고 있는 것을 의미한다.

[0023] 구해진 p-value에 대하여, p-value= α의 경우를 「석세스」라고 한다. 이것을 m샘플에 대하여 행하고, 그 석세스율과 p-value의 일양성을 평가한다. p-value가 일양(一樣)이며, 또한 석세스율이 1-α를 중심으로 하는 특

정한 범위에 들어가 있는 경우에 테스트를 「패스한다」라고 한다. 초기값(CA코어에 주어지는 시크릿키)에 대하여 다소 테스트의 결과가 상이하므로, 각 테스트에 대하여 몇개의 초기값으로 테스트한다. 이하의 예에서는, $n= 10^6$, $\alpha= 0.01$, $m= 1000$를 사용하였다. 각 테스트에서 사용한 파라미터를 도 5에 나타낸다.

[0024] 도 6은, RC4(256)비트키)의 테스트 결과를 나타내고, 도 7은, CA를 30의 테스트 결과를 나타낸다. 각 도면은, 초기값을 다르게 하여 얻어진 2개의 테스트 결과를 나타내고 있다. 테스트 결과를 나타낸 그래프에 있어서, 가로축은, 테스트의 종류, 세로축은 석세스율을 나타내고, 상하의 선으로 둘러싸인 영역이 패스 영역이다. 또, CA의 경우, 셀 번호를 고정하여 시간 방향으로 비트열을 샘플링했다. 셀수는, 예를 들면 1000이다.

[0025] 도 6으로부터 알 수 있는 바와 같이, RC4에서는, 모든 테스트에서 p-value의 일양성은, 패스하지만, 7번째의 테스트 항목(Non-overlapping Template Matching Test의 하나의 template에 대하여만 항상 석세스율이 범위로부터 벗어나는 문제가 있다. 7번째의 테스트에서는, 148종류의 template를 사용하여 패턴 매칭하고, 각종 류에 대한 석세스율이 계산된다. 또, 초기값에에서는, 10번째의 테스트 항목(Lempel Ziv Compression)도 빠지고 있다. 이와 같이, RC4는, 몇개의 테스트를 패스하지 못하는 문제가 있다.

[0026] 도 7로부터 알 수 있는 바와 같이, CA 를 30에서는, 초기값에 따라서는, 3번째의 테스트 항목(Runs Test), 15번째의 테스트 항목(Random Excursions), 16번째의 테스트 항목(Random Excursions Variant)이 패스하지 못하는 문제가 있다. 그보다도 심각한 것은, 10번째의 테스트 항목(Lempel Ziv Compression)의 p-value의 일양성이 상실되어 있는 것이다. 이것은, 비트열의 특징에 편향이 있는 것을 의미하고 있고, 그로부터 랜덤열과의 구별을 할 가능성이 있어 문제이다

[0027] 또, 1타임 스텝에서 1비트의 정보 밖에 사용할 수 없다는 제약이 있으므로, 셀수(게이트수)가 증가해도 암호화의 처리 속도를 고속으로 할 수 없다는 문제가 있었다.

[0028] 따라서, 본 발명의 목적은, CA를 사용한 경우에, 모든 테스트를 패스할 수 있고, 랜덤성이 우수하고, 또 암호화의 처리 속도를 향상시키는 것이 가능한 난수 생성, 암호화 및 복호를 위한 장치, 방법, 프로그램, 및 기록 매체를 제공하는 것에 있다.

발명의 상세한 설명

[0029] 청구의 범위 1의 발명은, 1차원적으로 복수개의 셀이 배치되고, 각 셀이 상태값으로서 0이나 1을 가지고, 다음 시각에서의 각 셀의 상태값은 자체의 상태값과 근방의 셀 상태값에만 의존하는 룰에 의해 주어지고, 각 셀의 상태값은 상기 룰에 의해 갱신되는 1차원 2상태 K근방 셀 오토맨에 의한 난수 생성 장치에 있어서,

[0030] 복수개의 셀 중 적어도 하나의 셀의 출력을 출력하고, 복수개의 셀의 다음 시각의 상태값을 갱신하기 위해, 현재 시각의 복수개의 셀의 출력을 입력으로 피드백하는 경로와,

[0031] 경로에 삽입되고, 복수개의 셀의 출력을 소정의 셀수 시프트하는 시프트 처리 수단을 구비한 난수 생성 장치이다.

[0032] 청구의 법위 6의 발명은, 복수개의 셀의 각 셀이 상태값으로서 0이나 1을 가지고, 다음 시각에서의 각 셀의 상태값은 자체의 상태값과 근방의 셀 상태값에만 의존하는 룰에 의해 주어지고, 각 셀의 상태값은 상기 룰에 의해 갱신되는 1차원 2상태 K근방 셀 오토맨에 의한 난수 생성 방법에 있어서,

[0033] 복수개의 셀 중 적어도 하나의 셀의 출력을 출력하고, 복수개의 셀의 다음 시각의 상태값을 갱신하기 위해, 현재 시각의 복수개의 셀의 출력을 입력으로 피드백할 때, 복수개의 셀의 출력을 소정의 셀수 시프트하는 난수 생성 방법이다.

[0034] 청구의 범위 10의 발명은, 컴퓨터에 대하여, 복수개의 셀의 각 셀이 상태값으로서 0이나 1을 가지고, 다음 시각에서의 각 셀의 상태값은 자체의 상태값과 근방의 셀 상태값에만 의존하는 룰에 의해 주어지고, 각 셀의 상태값은 상기 룰에 의해 갱신되는 1차원 2상태 K근방 셀 오토맨에 의한 난수 생성 방법을 실행하도록 하기 위한 프로그램에 있어서,

[0035] 복수개의 셀 중 적어도 하나의 셀의 출력을 출력하고, 복수개의 셀의 다음 시각의 상태값을 갱신하기 위해, 현재 시각의 복수개의 셀의 출력을 입력으로 피드백할 때, 복수개의 셀의 출력을 소정의 셀수 시프트하는 난수 생성 방법을 실행하도록 하기 위한 프로그램이다.

[0036] 청구의 범위 11의 발명은, 난수 생성 방법을 실행하도록 하기 위한 프로그램이 기록된, 컴퓨터로 판독 가능한

기록 매체이다.

[0037] 청구의 범위 12의 발명은, 평문과 난수의 배타적 논리합에 의해 암호문을 생성하는 암호화 장치에 있어서,

[0038] 난수는, 1차원적으로 복수개의 셀이 배치되고, 각 셀이 상태값으로서 0이나 1을 가지고, 다음 시각에서의 각 셀의 상태값은 자체의 상태값과 근방의 셀 상태값에만 의존하는 룰에 의해 주어지고, 각 셀의 상태값은 상기 룰에 의해 갱신되는 1차원 2상태 K근방 셀 오토맨에 의한 난수 생성 장치에 의해 생성되고,

[0039] 복수개의 셀 중 적어도 하나의 셀의 출력을 출력하고, 복수개의 셀의 다음 시각의 상태값을 갱신하기 위해, 현재 시각의 복수개의 셀의 출력을 입력으로 피드백하는 경로와,

[0040] 경로에 삽입되고, 복수개의 셀의 출력을 소정의 셀수 시프트하는 시프트 처리 수단을 구비한 것을 특징으로 하는 암호화 장치이다.

[0041] 청구의 범위 17의 발명은, 평문과 난수의 배타적 논리합에 의해 암호문을 생성하는 암호화 방법에 있어서,

[0042] 난수는, 복수개의 셀의 각 셀이 상태값으로서 0이나 1을 가지고, 다음 시각에서의 각 셀의 상태값은 자체의 상태값과 근방의 셀 상태값에만 의존하는 룰에 의해 주어지고, 각 셀의 상태값은 상기 룰에 의해 갱신되는 1차원 2상태 K근방 셀 오토맨에 의한 난수 생성 방법에 의해 생성되고,

[0043] 난수 생성 방법은, 복수개의 셀 중 적어도 하나의 셀의 출력을 출력하고, 복수개의 셀의 다음 시각의 상태값을 갱신하기 위해, 현재 시각의 복수개의 셀의 출력을 입력으로 피드백할 때, 복수개의 셀의 출력을 소정의 셀수 시프트하는 것을 특징으로 하는 암호화 방법이다.

[0044] 청구의 범위 21의 발명은, 컴퓨터에 대하여, 평문과 난수의 배타적 논리합에 의해 암호문을 생성하는 암호화 방법을 실행하도록 하기 위한 프로그램에 있어서,

[0045] 난수는, 복수개의 셀의 각 셀이 상태값으로서 0이나 1을 가지고, 다음 시각에서의 각 셀의 상태값은 자체의 상태값과 근방의 셀 상태값에만 의존하는 룰에 의해 주어지고, 각 셀의 상태값은 상기 룰에 의해 갱신되는 1차원 2상태 K근방 셀 오토맨에 의한 난수 생성 방법에 의해 생성되고,

[0046] 난수 생성 방법은, 복수개의 셀 중 적어도 하나의 셀의 출력을 출력하고, 복수개의 셀의 다음 시각의 상태값을 갱신하기 위해, 현재 시각의 복수개의 셀의 출력을 입력으로 피드백할 때, 복수개의 셀의 출력을 소정의 셀수 시프트하는 것을 특징으로 하는 암호화 방법을 실행하도록 하기 위한 프로그램이다.

[0047] 청구의 범위 22의 발명은, 암호화 방법을 실행하도록 하기 위한 프로그램이 기록된, 컴퓨터로 판독 가능한 기록 매체이다.

[0048] 청구의 범위 23의 발명은, 암호문과 난수의 배타적 논리합에 의해 암호문을 복호하는 복호 장치에 있어서,

[0049] 난수는, 1차원적으로 복수개의 셀이 배치되고, 각 셀이 상태값으로서 0이나 1을 가지고, 다음 시각에서의 각 셀의 상태값은 자체의 상태값과 근방의 셀 상태값에만 의존하는 룰에 의해 주어지고, 각 셀의 상태값은 상기 룰에 의해 갱신되는 1차원 2상태 K근방 셀 오토맨에 의한 난수 생성 장치에 의해 생성되고,

[0050] 복수개의 셀 중 적어도 하나의 셀의 출력을 출력하고, 복수개의 셀의 다음 시각의 상태값을 갱신하기 위해, 현재 시각의 복수개의 셀의 출력을 입력으로 피드백하는 경로와,

[0051] 경로에 삽입되고, 복수개의 셀의 출력을 소정의 셀수 시프트하는 시프트 처리 수단을 구비한 것을 특징으로 하는 복호 장치이다.

[0052] 청구의 범위 26의 발명은, 암호문과 난수의 배타적 논리합에 의해 암호문을 복호하는 복호 방법에 있어서,

[0053] 난수는, 복수개의 셀의 각 셀이 상태값으로서 0이나 1을 가지고, 다음 시각에서의 각 셀의 상태값은 자체의 상태값과 근방의 셀 상태값에만 의존하는 룰에 의해 주어지고, 각 셀의 상태값은 상기 룰에 의해 갱신되는 1차원 2상태 K근방 셀 오토맨에 의한 난수 생성 방법에 의해 생성되고,

[0054] 난수 생성 방법은, 복수개의 셀 중 적어도 하나의 셀의 출력을 출력하고, 복수개의 셀의 다음 시각의 상태값을 갱신하기 위해, 현재 시각의 복수개의 셀의 출력을 입력으로 피드백할 때, 복수개의 셀의 출력을 소정의 셀수 시프트하는 것을 특징으로 하는 복호 방법이다.

[0055] 청구의 범위 28의 발명은, 컴퓨터에 대하여, 암호문과 난수의 배타적 논리합에 의해 암호문을 복호하는 복호 방법을 실행하도록 하기 위한 프로그램에 있어서,

[0056] 난수는, 복수개의 셀의 각 셀이 상태값으로서 0이나 1을 가지고, 다음 시각에서의 각 셀의 상태값은 자체의 상태값과 근방의 셀 상태값에만 의존하는 룰에 의해 주어지고, 각 셀의 상태값은 상기 룰에 의해 갱신되는 1차원 2상태 K근방 셀 오토맨에 의한 난수 생성 방법에 의해 생성되고,

[0057] 난수 생성 방법은, 복수개의 셀 중 적어도 하나의 셀의 출력을 출력하고, 복수개의 셀의 다음 시각의 상태값을 갱신하기 위해, 현재 시각의 복수개의 셀의 출력을 입력으로 피드백할 때, 복수개의 셀의 출력을 소정의 셀수 시프트하는 것을 특징으로 하는 복호 방법을 실행하도록 하기 위한 프로그램이다.

[0058] 청구의 범위 29의 발명은, 복호 방법을 실행하도록 하기 위한 프로그램이 기록된, 컴퓨터로 판독 가능한 기록 매체이다.

실 시 예

[0071] 도 8 (A)는, 본 발명의 기본적 구성을 나타낸다. 입력 정보 데이터(평문)가 M비트의 병렬 데이터로 변환되어 EX-OR 게이트(11)에 입력된다. CA코어(12)로부터의 M비트의 병렬 데이터의 키스트림이 EX-OR 게이트(11)의 다른 쪽의 입력으로 되고, EX-OR 게이트(11)로부터 암호문이 출력된다. CA코어(12)에 대해에서는, 초기값으로서의 시크릿키의 데이터와 클록이 입력되고, 40비트 병렬의 난수 데이터(키스트림)가 생성된다. 도 8 (B)는, 일례로서, M= 40으로 한 경우의 일실시예를 나타낸다. CA코어(12)는, 전술한 1차원 2상태 3근방 셀 오토맨의 구성으로 되고, 식(2) 또는 식(3)에 나타낸 바와 같은 룰 30에 따라 상태 갱신이 행해지는 것이다.

[0072] 복호기(도시하지 않음)의 구성은, 전술한 암호화기와 마찬가지로 구성된다. 즉, 암호문이 EX-OR 게이트에 공급되고, 키스트림이 EX-OR 게이트에 공급되는 것에 따라서 복호 처리가 된다. 초기값을 공통으로 하여, 동기를 취함으로써 암호화와 복호로, 공통의 키가 사용된다.

[0073] 도 9는, 일실시예(3근방 CA, 셀수 1000)에 있어서의 CA코어(12)의 구성의 일례를 나타낸다. S1, S2, S3, … …, S999, S1000은, 각각 제1 번째로부터 제1000번째의 셀을 나타낸다. 각 셀에 대하여는, 자체와 양 옆의 셀에 대한 합계 3개의 입력이 공급된다. 제1 번의 셀 S1에 대한 좌측 인접한 셀에 대한 입력으로서, 셀 S1000에 대한 입력이 사용되어 제1000번째의 셀 S1000에 대한 우측 인접한 셀에 대한 입력으로서, 셀 S1에 대한 입력이 사용된다. 각 셀은, 전술한 식(2) 또는 식(3)으로 표현되는 논리 연산을 행하고, 논리 연산 결과 O1~ O1000를 출력한다.

[0074] 셀 S1~S1000에는, 각각 레지스터가 포함되고, 각 레지스터가 클록(도시하지 않음)에 동기하여 논리 연산 결과를 차례로 취하여, 유지하는 구성으로 되어 있다. 타임 스텝 t에 있어서의 논리 연산 결과가 셀 S1~S1000로부터 출력되면 각 셀에 있어서 연산된 다음의 타임 스텝 t+1의 논리 연산 결과가 레지스터에 받아들여지게 된다.

[0075] 셀 S1~S1000의 출력 O1~ O1000이 다음의 타임 스텝의 연산을 위해, 셀 S1~S1000에 대하여 피드백 되지만, 그 경우에, 로테이션 시프트부(13)에 의해 로테이션 시프트 조작이 행해진다. 로테이션 시프트 조작은, 출력 O1~O1000을 전체적으로 도면을 향해 볼 때 좌측으로 시프트시켜 셀에 피드백하는 것이다. 일례로서, 11셀의 시프트가 행해진다. 이 경우에는, 가장 좌측단의 셀 S1에 대하여, 출력 O12가 입력되고, 좌측으로부터 2번째의 셀 S2에 대하여, 출력 O13가 입력된다. 이하, 11셀 분의 시프트가 행해져 피드백된다. 또, 셀 S1의 좌측 상의 출력 O1~O11은, 우측의 11개의 셀 S990~S1000에 대하여 입력된다.

[0076] 그리고, 로테이션 시프트의 방향은, 도면을 향해 보아 좌측으로 하였으나, 반대의 우측으로 로테이션 시프트 해도 된다. 또, 로테이션 시프트량은, 설정된 후에 바꿀 필요가 없기 때문에, 로테이션 시프트(13)는, 결선의 방법에 의해 구성할 수 있다. 단, 로테이션 시프트량의 설정의 변경을 가능하게 하기 위해, 스위칭 회로에 의해 로테이션 시프트부(13)를 구성해도 된다.

[0077] 셀 S1~S1000의 출력 O1~O1000 중 하나의 출력을 1비트의 키스트림해 선택하여 암호키로서 사용할 수 있다. 일실시예에서는, 다수개 비트의 키스트림으로서 출력하기 위해, 셀 S1~S1000의 출력 O1~O1000가 샘플링부(14)에 공급된다. 샘플링부(14)는, 출력 O1~O1000 중 M비트를 키스트림으로서 선택한다. 샘플링되는 셀 번호는, 등간격이 아니고, 선택되는 셀 번호의 간격이 서서히 커지도록 된다. 예를 들면 N= 1000, M= 40의 경우, 1, 7, 14, 22, 31, 41, 52, 64, …, 976과 간격이 1씩 증가하도록 된다.

[0078] 일반적으로, n번째(n>1)의 셀 번호 a(n)는,하기의 식(4)에 나타낸 것으로 된다. 전술한 예의 경우, 파라미터는, a(1)=1, d= 6이다.

$$a(n)=a(1)+\sum_{m=1}^{n-1}(d+m-1) \qquad (4)$$

[0079]

[0080] 그리고, 샘플링의 방법은, 설정된 후에 바꿀 필요가 없기 때문에, 샘플링부(14)는, 유효한 출력선을 설정하는 것만으로 구성할 수 있다. 단, 샘플링의 방법의 설정의 변경을 가능하게 하기 위해, 스위칭 회로에 의해 샘플링부(14)를 구성해도 된다. 또, 샘플링되는 셀 번호의 간격이 서서히 커지도록 했지만, 서서히 작아지도록 해도 된다. 또, 랜덤에 셀의 간격이 변화되는 것이라도 된다.

[0081] 도 10은, 전술한 일실시예에 있어서 샘플링부(14)로부터 출력되는 키스트림을 나타낸 것이다. 최초의 타임 스텝(t= 1)에서는, 원래의 CA로부터 보면, 셀 번호의 1,7,14,22,31, …가 키스트림으로서 선택되어 출력된다. 로테이션 시프트 처리가 행해지므로, 다음의 타임 스텝(t= 2)에서는, 원래의 CA로부터 보면, 셀 번호의 12,18,25,33 …이 키스트림으로서 선택되어 출력된다.

[0082] 도 11은, 전술한 본 발명의 일실시예에 있어서, 로테이션 시프트부(13)만을 가지고, 샘플링부(14)를 가지고 있지 않은 경우의 NIST 테스트의 결과를 나타낸다. 도 12는, 로테이션 시프트부(13) 및 샘플링부(14)의 양쪽을 가지는 경우의 NIST 테스트의 결과를 나타낸다.

[0083] 로테이션 시프트수를 11로 한 경우의 테스트 결과(도 11)로부터 알 수 있는 바와 같이, 2개의 초기값에 대하여 16종류의 모든 테스트를 패스할 수 있다.

[0084] 또, 셀수가 1000이며, 샘플링에 의해 40셀의 정보를 추출한 경우의 테스트 결과(도 12)에서는, 초기값에 따라서는, 7번째의 테스트(Non-overlapping Template Matching Test) 중 하나의 패턴이 패스하고 있지 않지만, 항상 패스하지 못하는 것은 아니기 때문에 문제는 없다.

[0085] 셀수 1000의 CA를 30(로테이션 시프트수 11셀)을 FPGA(Field Programmable Gate Array: 대규모 PLD(Programmable logic Device)에 실장한 결과, (게이트수= 14699), 최대 동작 주파수= 105.831MHz, 암호화(복호)속도 4.233Gbps)의 결과를 얻을 수 있었다. 예를 들면 디지털 비디오 데이터의 리얼타임 암호화 및 복호에서는, 클록의 주파수가 27MHz이며, 약(1Gbps의 암호(복호)화 속도를 달성할 수 있었다.

산업상 이용 가능성

[0086] 전술한 본 발명에 의하면, 먼저 제안되어 있는 RC4 및 룰 30과 비교하여 랜덤성을 보다 향상시키는 것이 가능하다. 또, 안전성을 손상시키지 않고, 다수개 비트의 난수를 꺼낼 수 있으므로, 암호화의 속도를 향상시키는 것이 가능해진다. 또한, 회로 구성이 단순하므로, 최대 동작 주파수를 높게 할 수 있다. 즉, 대량의 정보를 고속으로 처리하는 하드웨어를 용이하게 실현할 수 있다.

[0087] 본 발명은, 전술한 실시예에 한정되지 않고, 본 발명의 요지를 벗어나지 않는 범위 내에서 각종의 변형이나 응용이 가능하다. 예를 들면 본 발명은, 일반적으로 K개의 셀 상태값에 의존하는 1차원 2상태 K근방의 셀 오토맨을 사용할 수 있다. 또, 본 발명에 의한 난수 생성기는, 스트림 암호 이외에 몬테카를로법(Monte Carlo method)에 대하여도 적용할 수 있다.

도면의 간단한 설명

[0059] 도 1은, 종래의 블록 암호 및 스트림 암호의 개략을 설명하기 위한 약선도이다.

[0060] 도 2는, 종래의 CA를 사용한 암호화기의 구성을 나타낸 블록도이다.

[0061] 도 3은, 종래의 CA를 사용한 암호화기에 있어서의 키스트림의 설명을 위한 약선도이다.

[0062] 도 4는, 암호용의 난수로서의 평가의 통계 테스트의 일례의 테스트 항목을 나타낸 약선도이다.

[0063] 도 5는, 암호용의 난수로서의 평가의 통계 테스트의 일례의 파라미터를 나타낸 약선도이다.

[0064] 도 6은, 종래의 스트림 암호인 RC4의 통계 테스트의 결과의 일례 및 다른 예를 나타낸 약선도이다.

[0065] 도 7은, 종래의 CA를 사용한 암호의 통계 테스트의 결과의 일례 및 다른 예를 나타낸 약선도이다.

[0066] 도 8은, 본 발명에 의한 암호화기의 기본 구성 및 일실시예를 나타낸 블록도이다.

[0067] 도 9는, 본 발명에 의한 암호화기의 일실시예를 나타낸 블록도이다.

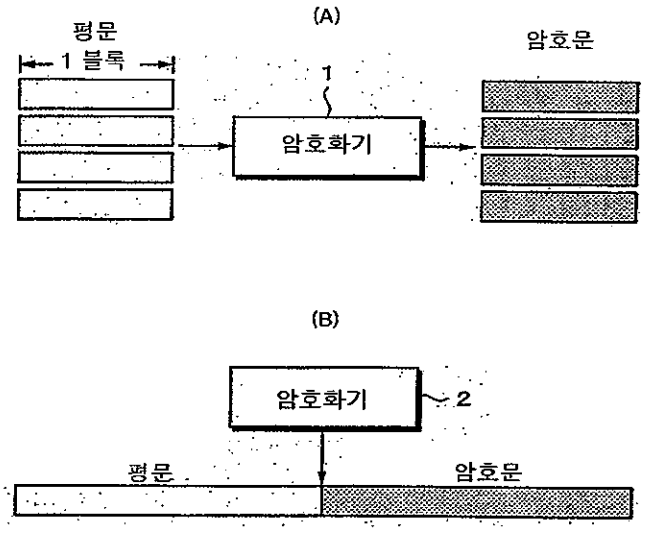
[0068] 도 10은, 본 발명에 의한 암호화기의 일실시예에 있어서의 키스트림의 설명을 위한 약선도이다.

[0069] 도 11은, 로테이션 시프트를 행하는 본 발명의 통계 테스트의 결과의 일례 및 다른 예를 나타낸 약선도이다.

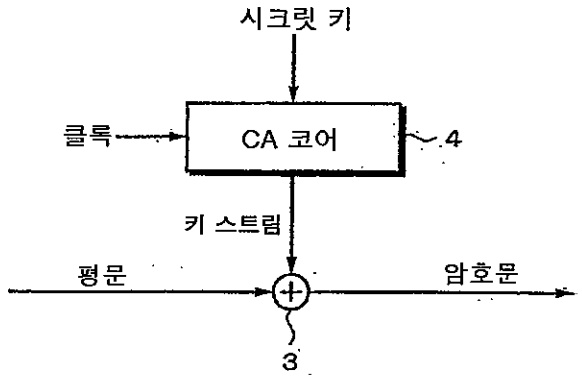
[0070] 도 12는, 본 발명의 일실시예의 통계 테스트의 결과의 일례 및 다른 예를 나타낸 약선도이다.

도면

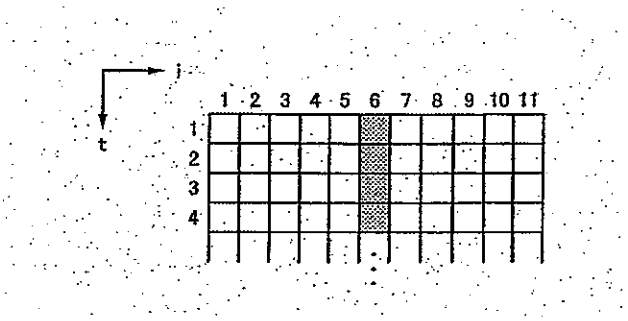
도면1



도면2



도면3



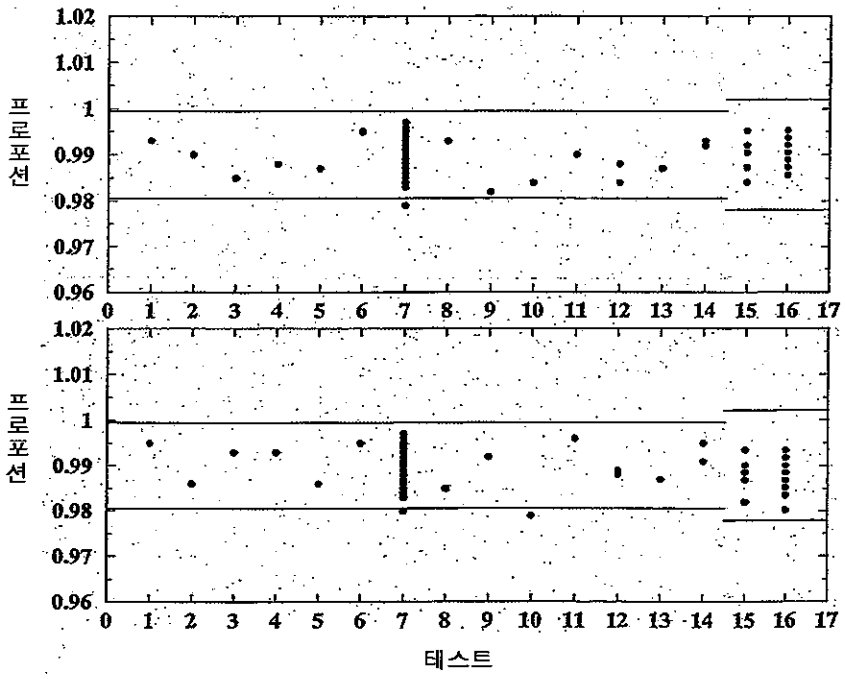
도면4

번호	테스트명
1	Frequency
2	Block Frequency
3	Runs
4	Longest Run
5	Binary Matrix Rank
6	Discrete Fourier Transform
7	Non-overlapping Template Matching
8	Overlapping Template Matching
9	Universal
10	Lempel Ziv Compression
11	Linear Complexity
12	Serial
13	Approximate Entropy
14	Cumulative Sums
15	Random Excursions
16	Random Excursions Variant

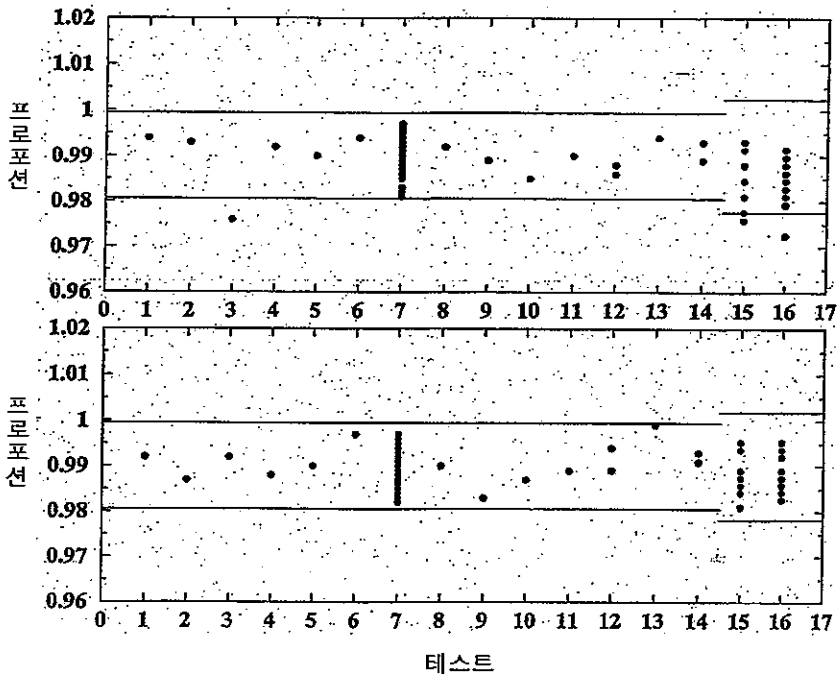
도면5

테스트명	블록 길이
Block Frequency	20,000
Non-overlapping Template Matching	9
Overlapping Template Matching	9
Universal (Initialization Steps)	7 (1280)
Linear Complexity	500
Serial	10
Approximate Entropy	10

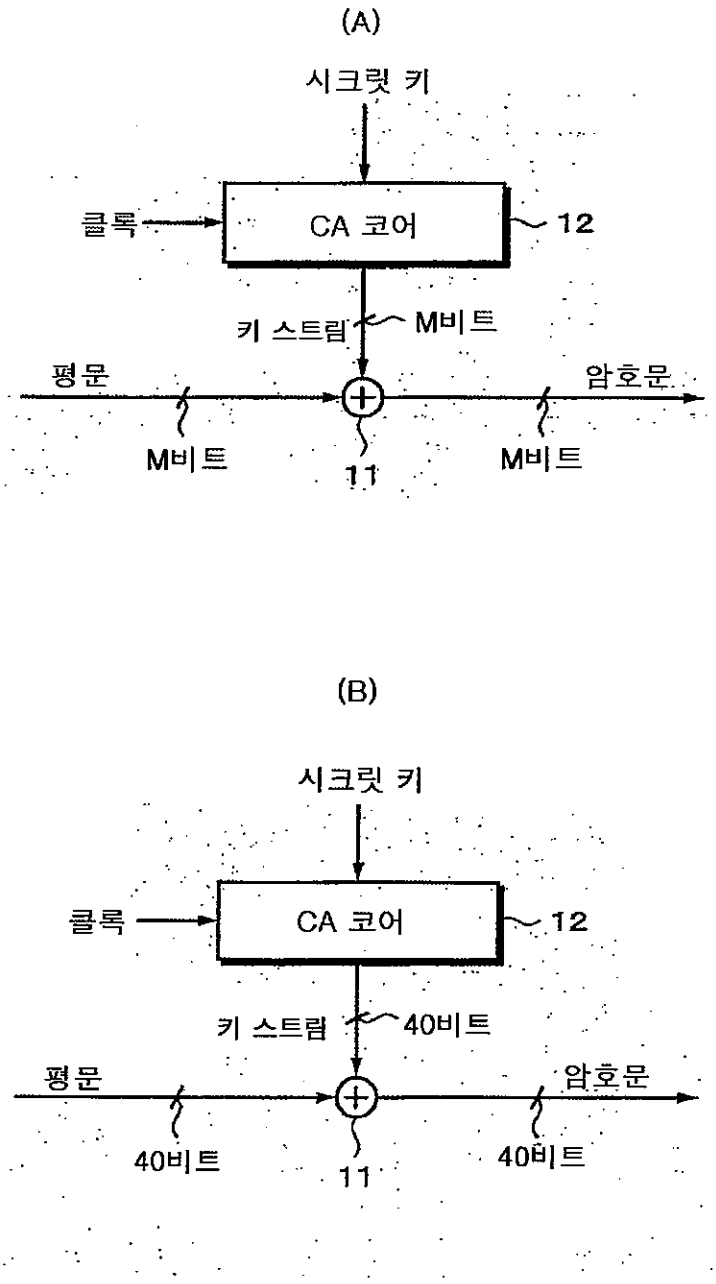
도면6


프로포션
1.02
1.01
1
0.99
0.98
0.97
0.96
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
프로포션
테스트

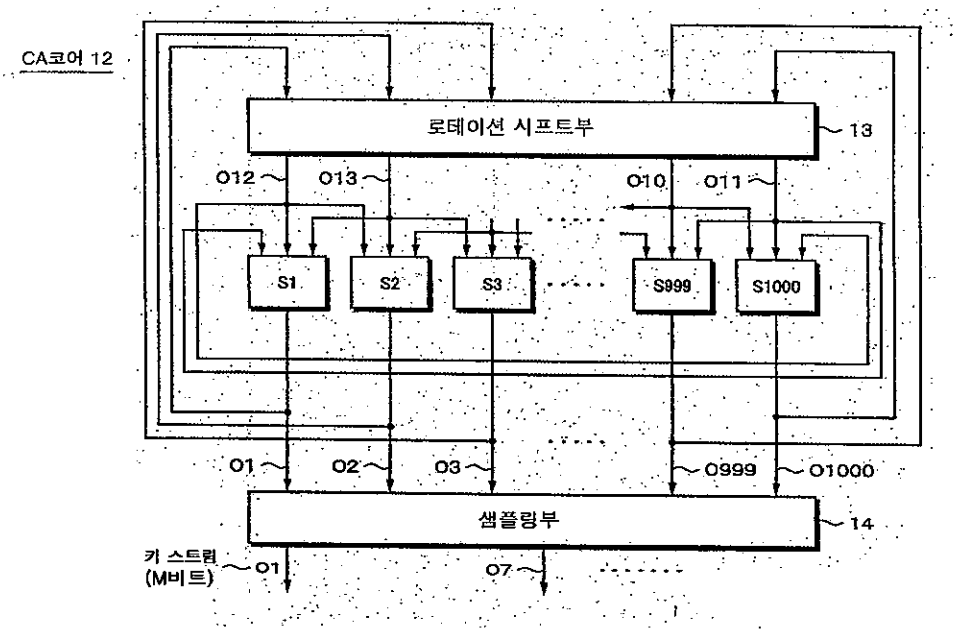
도면7


프로포션
1.02
1.01
1
0.99
0.98
0.97
0.96
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
프로포션
테스트

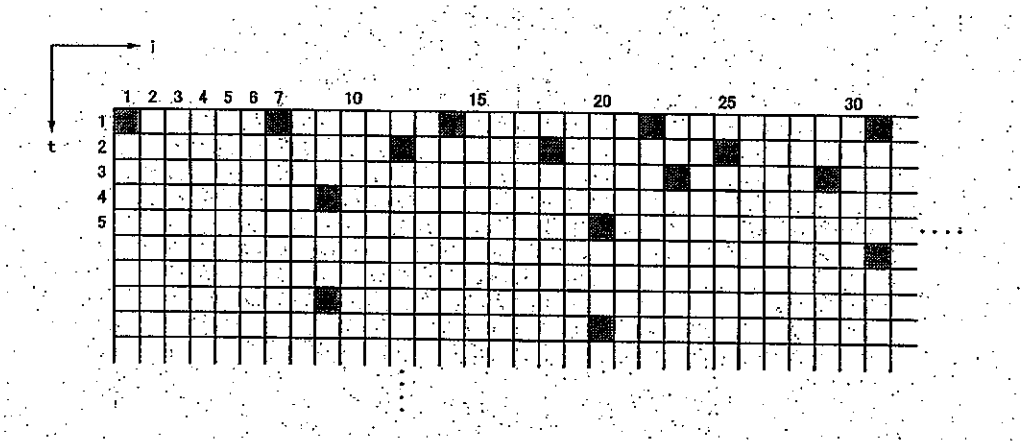
도면8


(A)
시크릿 키
클록
CA 코어
12
키 스트림
M비트
평문
암호문
M비트
11
M비트
(B)
시크릿 키
클록
CA 코어
12
키 스트림
40비트
평문
암호문
40비트
11
40비트

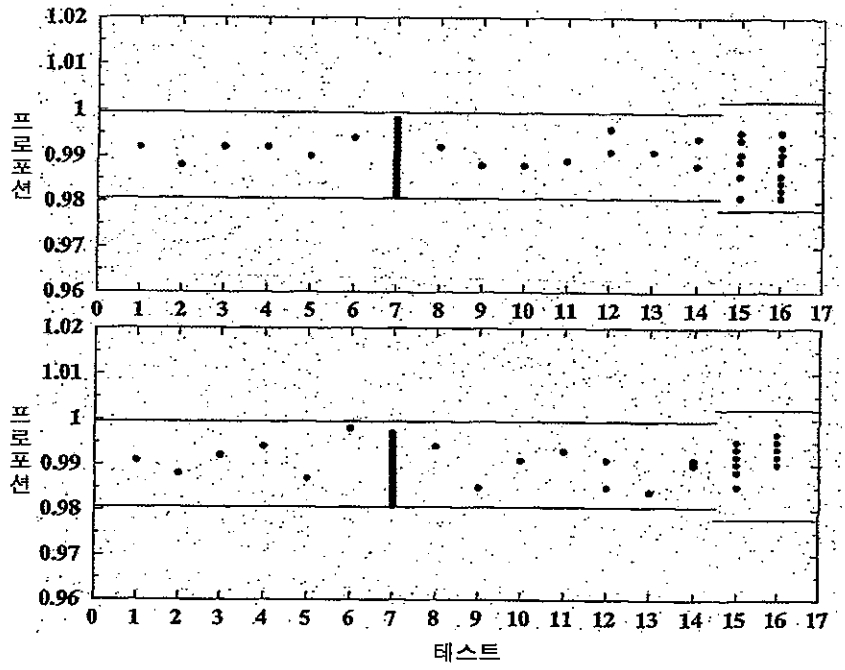
도면9


CA코어 12
로테이션 시프트부
13
O12
O13
O10
O11
S1
S2
S3
S999
S1000
O1
O2
O3
O999
O1000
샘플링부
14
키 스트림
(M비트)
O1
O7

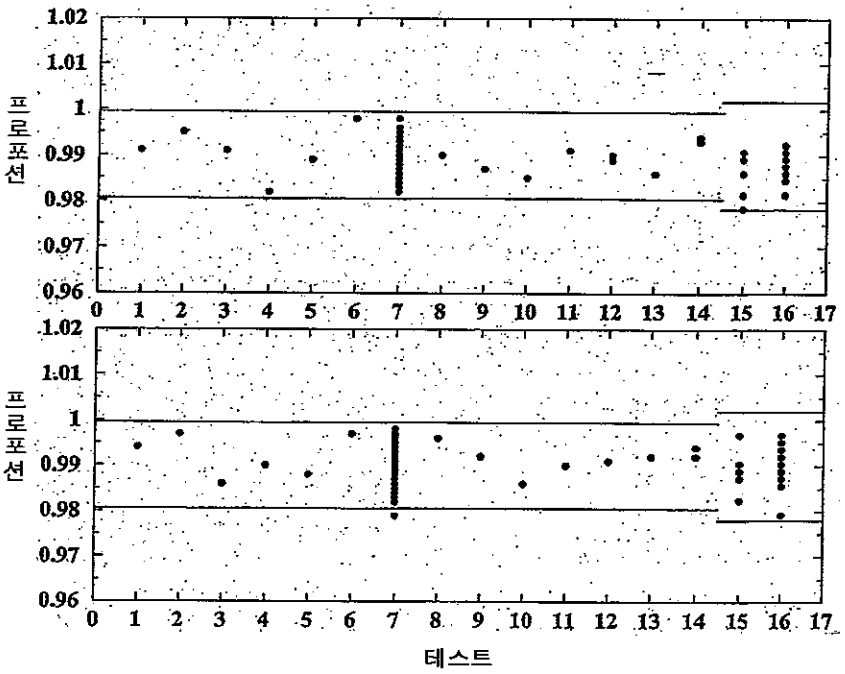
도면10


i
t
1 2 3 4 5 6 7 10 15 20 25 30
1
2
3
4
5

도면11


1.02
1.01
1
0.99
0.98
0.97
0.96
프로포션
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
테스트

도면12


1.02
1.01
1
0.99
0.98
0.97
0.96
프로포션
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
테스트