(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2021년04월23일
(11) 등록번호 10-2243889
(24) 등록일자 2021년04월19일

(51) 국제특허분류(Int. Cl.)
*H03M 13/37* (2006.01) *H03M 13/00* (2017.01)
(52) CPC특허분류
*H03M 13/3707* (2013.01)
*H03M 13/617* (2013.01)
(21) 출원번호 10-2019-0167172
(22) 출원일자 2019년12월13일
심사청구일자 2019년12월13일
(56) 선행기술조사문헌
US20130244642 A1

(73) 특허권자
**국방과학연구소**
대전광역시 유성구 북유성대로488번길 160 (수남동)
(72) 발명자
**박철순**
대전광역시 유성구 북유성대로488번길 160
**이치호**
대전광역시 유성구 북유성대로488번길 160
*(뒷면에 계속)*
(74) 대리인
**제일특허법인(유), 박장원**

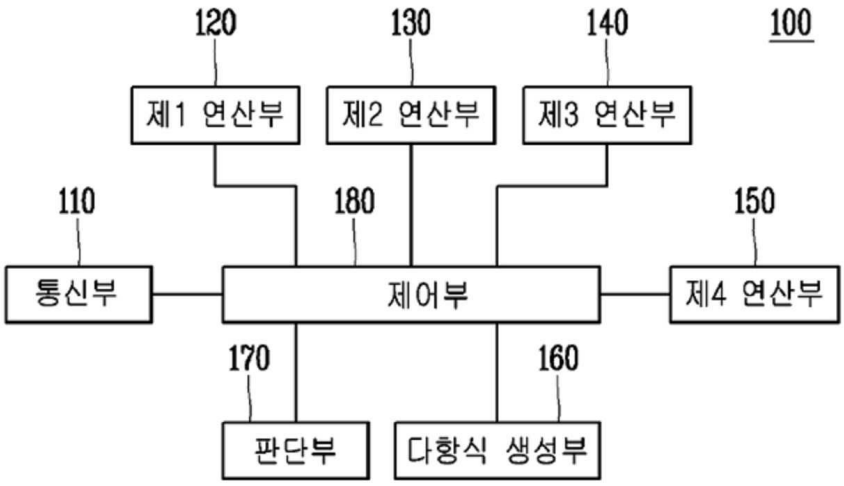
전체 청구항 수 : 총 11 항 심사관 : 조춘근

(54) 발명의 명칭 **데이터 복호화 장치 및 방법**

## (57) 요 약

본 발명은 데이터 복호화 장치 및 방법에 관한 것으로, 데이터가 암호화된 비트신호를 수신하는 통신부; 상기 데이터의 암호화에 사용된 확산코드의 길이에 대응하는 제1길이 만큼 상기 비트신호에 대한 비트 이동을 수행해 제1 연산스트림을 생성하는 제1 연산부; 상기 비트신호와 상기 제1 연산스트림을 이용하여 상기 확산코드가 상쇄된 제2 연산스트림을 생성하는 제2 연산부; 상기 제2 연산스트림에 대하여 제2 길이만큼 비트 이동을 수행해 제3 연산스트림을 생성하는 제3 연산부; 상기 제2 연산스트림과 상기 제3 연산스트림을 이용하여 상기 데이터가 상쇄된 제4 연산스트림을 생성하는 제4 연산부; 및 상기 제4 연산스트림을 이용하여 암호화된 상기 데이터를 복호화할 수 있는 생성다항식을 생성하는 다항식 생성부를 포함한다.

*대 표 도* - 도1



(52) CPC특허분류
*H03M 13/6516* (2013.01)
(72) 발명자
**정운섭**
대전광역시 유성구 북유성대로488번길 160
**김동영**
서울특별시 성동구 왕십리로 222
**송정환**
서울특별시 성동구 왕십리로 222
**윤동원**
서울특별시 성동구 왕십리로 222

# 명 세 서

## 청구범위

### 청구항 1

데이터가 암호화된 비트신호를 수신하는 통신부;

상기 데이터의 암호화에 사용된 확산코드의 길이에 대응하는 제1길이 만큼 상기 비트신호에 비트 이동을 수행해 제1 연산스트림을 생성하는 제1 연산부;

상기 비트신호와 상기 제1 연산스트림을 이용하여 상기 확산코드가 상쇄된 제2 연산스트림을 생성하는 제2 연산부;

상기 제2 연산스트림에 대하여 제2 길이만큼 비트 이동을 수행해 제3 연산스트림을 생성하는 제3 연산부;

상기 제2 연산스트림과 상기 제3 연산스트림을 이용하여 상기 데이터가 상쇄된 제4 연산스트림을 생성하는 제4 연산부; 및

상기 제4 연산스트림을 이용하여 암호화된 상기 데이터를 복호화할 수 있는 생성다항식을 생성하는 다항식 생성부를 포함하는 데이터 복호화 장치.

### 청구항 2

제1항에 있어서,

상기 생성다항식을 이용하여 상기 비트신호를 복호화하고, 복호화 가능 여부를 판단하는 판단부를 더 포함하는 것을 특징으로 하는 데이터 복호화 장치.

### 청구항 3

제1항에 있어서,

상기 제1 연산부 및 상기 제3 연산부는

왼쪽 시프트 연산자를 통해 비트 이동을 수행하는 것을 특징으로 하는 데이터 복호화 장치.

### 청구항 4

제1항에 있어서,

상기 제1 길이는,

상기 확산코드가 가질 수 있는 복수의 비트수들 중 어느 하나이고,

상기 제2 길이는,

1 이상의 자연수인 것을 특징으로 하는 데이터 복호화 장치.

### 청구항 5

제1항에 있어서,

상기 제2 연산부는,

상기 비트신호와 상기 제1 연산스트림 간의 배타적 논리합(Exclusive OR)을 수행하여 상기 확산코드를 상쇄하고,

상기 제4 연산부는,

상기 제2 연산스트림과 상기 제3 연산스트림 간의 배타적 논리합(Exclusive OR)을 수행하여 상기 데이터를 상쇄하는 것을 특징으로 하는 데이터 복호화 장치.

**청구항 6**

데이터가 암호화된 비트신호를 수신하는 단계;

상기 데이터의 암호화에 사용된 확산코드의 길이에 대응하는 제1길이 만큼 상기 비트신호에 비트 이동을 수행해 제1 연산스트림을 생성하는 단계;

상기 비트신호와 상기 제1 연산스트림을 이용하여 상기 확산코드가 상쇄된 제2 연산스트림을 생성하는 단계;

상기 제2 연산스트림에 대하여 제2 길이만큼 비트 이동을 수행해 제3 연산스트림을 생성하는 단계;

상기 제2 연산스트림과 상기 제3 연산스트림을 이용하여 상기 데이터가 상쇄된 제4 연산스트림을 생성하는 단계; 및

상기 제4 연산스트림을 이용하여 암호화된 상기 데이터를 복호할 수 있는 생성다항식을 생성하는 단계를 포함하는 데이터 복호화 방법.

**청구항 7**

제6항에 있어서,

상기 생성다항식을 이용하여 상기 비트신호를 복호화하고, 복호화 가능 여부를 판단하는 단계를 더 포함하는 것을 특징으로 하는 데이터 복호화 방법.

**청구항 8**

제7항에 있어서,

상기 복호화 가능 여부를 판단하는 단계에서, 상기 비트신호가 상기 생성다항식으로 복호화가 불가능한 것으로 판단되면,

상기 확산코드가 가질 수 있는 복수의 비트수 중 상기 제1 길이가 아닌 제3 길이만큼 상기 비트신호에 비트 이동을 수행해 제1-1 연산스트림을 생성하는 단계;

상기 비트신호와 상기 제1-1 연산스트림을 이용하여 상기 확산코드가 상쇄된 제2-1 연산스트림을 생성하는 단계;

상기 제2-1 연산스트림에 대하여 상기 제2 길이만큼 비트 이동을 수행해 제3-1 연산스트림을 생성하는 단계;

상기 제2-1 연산스트림과 상기 제3-1 연산스트림을 이용하여 상기 데이터가 상쇄된 제4-1 연산스트림을 생성하는 단계; 및

상기 제4-1 연산스트림을 이용하여 암호화된 상기 데이터를 복호할 수 있는 생성다항식을 생성하는 단계를 수행하는 데이터 복호화 방법.

**청구항 9**

제6항에 있어서,

상기 제1 연산스트림을 생성하는 단계 및 상기 제3 연산스트림을 생성하는 단계는,

왼쪽 시프트 연산자를 통해 비트 이동을 수행하는 것을 특징으로 하는 데이터 복호화 방법.

**청구항 10**

제6항에 있어서,

상기 제1 길이는,

상기 확산코드가 가질 수 있는 복수의 비트수들 중 어느 하나이고,

상기 제2 길이는,

1 이상의 자연수인 것을 특징으로 하는 데이터 복호화 방법.

**청구항 11**

제6항에 있어서,

상기 제2 연산스트림을 생성하는 단계는,

상기 비트신호와 상기 제1 연산스트림 간의 배타적 논리합(Exclusive OR)을 수행하여 상기 확산코드를 상쇄하고,

상기 제4 연산스트림을 생성하는 단계는,

상기 제2 연산스트림과 상기 제3 연산스트림 간의 배타적 논리합(Exclusive OR)을 수행하여 상기 데이터를 상쇄하는 것을 특징으로 하는 데이터 복호화 방법.

## *발명의 설명*

### *기 술 분 야*

[0001] 본 발명은 미상의 비트스트림의 암호화된 데이터를 복호화하는 데이터 복호화 장치 및 방법에 관한 것이다.

### *배 경 기 술*

[0002] 일반적으로 데이터 통신과정에 있어서, 송신장치는 전송할 데이터로 구성된 비트 블록을 스크램블링 시퀀스(Scrambling Sequence) 또는 생성다항식으로 스크램블 시킨 뒤 변조 과정을 거쳐 수신장치로 송신한다.

[0003] 수신장치는 수신된 신호의 복조 과정을 통하여 획득된 데이터 비트블록을 송신장치에서 사용된 것과 동일한 스크램블링 시퀀스 또느 생성다항식을 이용하여 디스크램블(Descramble)한다.

[0004] 스크램블링 과정은 데이터 비트 블록에 대한 간섭 신호의 영향을 랜덤화(Randomization)하기 위해 수행되며, 디스크램블링을 위해 송신장치와 수신장치는 동일한 스크램블링 시퀀스 또는 생성다항식 정보를 공유하여야 한다.

[0005] 스크램블링된 비트블록의 디스크램블링을 위해서는 스크램블링에 사용된 생성다항식이 요구되는데, 미상의 비트스트림을 수신하면 스크램블링에 사용된 생성다항식을 알지 못하므로 디스크램블링이 불가능하기에 생성다항식을 추정하는 방법이 요구된다.

## *발명의 내용*

### *해결하려는 과제*

[0006] 본 발명의 목적은 미상의 비트스트림에 사용된 생성다항식을 도출하여 암호화된 데이터를 복호화할 수 있는 데이터 복호화 장치 및 방법을 제공하는 것이다.

### *과제의 해결 수단*

[0007] 상기한 본 발명의 목적을 실현하기 위한 하나의 특징에 따른 데이터 복호화 장치는, 데이터가 암호화된 비트신호를 수신하는 통신부; 상기 데이터의 암호화에 사용된 확산코드의 길이에 대응하는 제1길이 만큼 상기 비트신호에 비트 이동을 수행해 제1 연산스트림을 생성하는 제1 연산부; 상기 비트신호와 상기 제1 연산스트림을 이용하여 상기 확산코드가 상쇄된 제2 연산스트림을 생성하는 제2 연산부; 상기 제2 연산스트림에 대하여 제2 길이 만큼 비트 이동을 수행해 제3 연산스트림을 생성하는 제3 연산부; 상기 제2 연산스트림과 상기 제3 연산스트림을 이용하여 상기 데이터가 상쇄된 제4 연산스트림을 생성하는 제4 연산부; 및 상기 제4 연산스트림을 이용하여 암호화된 상기 데이터를 복호화할 수 있는 생성다항식을 생성하는 다항식 생성부를 포함할 수 있다.

[0008] 그리고, 상기 생성다항식을 이용하여 상기 비트신호를 복호화하고, 복호화 가능 여부를 판단하는 판단부를 더 포함할 수 있다.

[0009] 또한, 상기 제1 연산부 및 상기 제3 연산부는, 왼쪽 시프트 연산자를 통해 비트 이동을 수행할 수 있다.

[0010] 그리고, 상기 제1 길이는, 상기 확산부호가 가질 수 있는 복수의 비트수들 중 어느 하나일 수 있고,

[0011] 상기 제2 길이는, 1 이상의 자연수일 수 있다.

[0012] 또한, 상기 제2 연산부는, 상기 비트신호와 상기 제1 연산스트림 간의 배타적 논리합(Exclusive OR)을 수행하여 상기 확산부호를 상쇄할 수 있고,

[0013] 상기 제4 연산부는, 상기 제2 연산스트림과 상기 제3 연산스트림 간의 배타적 논리합(Exclusive OR)을 수행하여 상기 메시지를 상쇄할 수 있다.

[0015] 한편, 상기한 본 발명의 목적을 실현하기 위한 다른 하나의 특징에 따른 데이터 복호화 방법은, 데이터가 암호화된 비트신호를 수신하는 단계; 상기 데이터의 암호화에 사용된 확산코드의 길이에 대응하는 제1길이 만큼 상기 비트신호에 비트 이동을 수행해 제1 연산스트림을 생성하는 단계; 상기 비트신호와 상기 제1 연산스트림을 이용하여 상기 확산코드가 상쇄된 제2 연산스트림을 생성하는 단계; 상기 제2 연산스트림에 대하여 제2 길이만큼 비트 이동을 수행해 제3 연산스트림을 생성하는 단계; 상기 제2 연산스트림과 상기 제3 연산스트림을 이용하여 상기 데이터가 상쇄된 제4 연산스트림을 생성하는 단계; 및 상기 제4 연산스트림을 이용하여 암호화된 상기 데이터를 복호할 수 있는 생성다항식을 생성하는 단계를 포함한다.

[0016] 그리고, 상기 생성다항식을 이용하여 상기 비트신호를 복호화하고, 복호화 가능 여부를 판단하는 단계를 더 포함할 수 있다.

[0017] 상기 복호화 가능 여부를 판단하는 단계에서, 상기 비트신호가 상기 생성다항식으로 복호화가 불가능한 것으로 판단되면, 상기 제1 연산스트림을 생성하는 단계를 수행할 수 있다.

[0018] 또한, 상기 제1 연산스트림을 생성하는 단계 및 상기 제3 연산스트림을 생성하는 단계는, 왼쪽 시프트 연산자를 통해 비트 이동을 수행할 수 있다.

[0019] 여기서, 상기 제1 길이는, 상기 확산부호가 가질 수 있는 복수의 비트수들 중 어느 하나일 수 있고,

[0020] 상기 제2 길이는, 1 이상의 자연수일 수 있다.

[0021] 그리고, 상기 제2 연산스트림을 생성하는 단계는, 상기 비트신호와 상기 제1 연산스트림 간의 배타적 논리합(Exclusive OR)을 수행하여 상기 확산부호를 상쇄할 수 있고,

[0022] 상기 제4 연산스트림을 생성하는 단계는, 상기 제2 연산스트림과 상기 제3 연산스트림 간의 배타적 논리합(Exclusive OR)을 수행하여 상기 메시지를 상쇄할 수 있다.

## *발명의 효과*

[0023] 본 발명의 실시예에 따른 데이터 복호화 장치 및 방법에 따르면,

[0024] 첫째, 미상의 비트신호의 암호화에 사용된 확산부호의 종류와 길이를 몰라도 생성다항식을 도출할 수 있다.

[0025] 둘째, 도출된 생성다항식을 이용하여 암호화된 메시지를 복호화할 수 있다.

## *도면의 간단한 설명*

[0026] 도 1은 본 발명의 일 실시예에 따른 데이터 복호화 장치를 개략적으로 나타낸 블럭도이다.

도 2는 본 발명의 일 실시예에 따른 데이터 복호화 방법을 설명하기 위한 흐름도이다.

도 3은 자기 동기 스크램블러의 구조를 개략적으로 나타낸 블럭도이다.

## *발명을 실시하기 위한 구체적인 내용*

[0027] 이하, 첨부한 도면들을 참조하여 본 발명의 바람직한 실시예를 보다 상세하게 설명한다. 이때, 첨부된 도면에서 동일한 구성 요소는 가능한 동일한 부호로 나타내고 있음에 유의한다. 또한, 본 발명의 요지를 흐리게 할 수 있는 공지 기능 및 구성에 대한 상세한 설명은 생략할 것이다. 마찬가지 이유로 첨부 도면에 있어서 일부 구성 요소는 과장되거나 생략되거나 개략적으로 도시되었다.

[0028] 도 1은 본 발명의 일 실시예에 따른 데이터 복호화 장치를 개략적으로 나타낸 블록도이다.

[0030] 도 1을 참조하면, 본 발명은 자기 동기 스크램블러로 데이터가 암호화된 비트신호의 복호화를 위해 비트신호의 생성에 사용된 생성다항식을 도출하고, 도출된 생성다항식을 이용하여 데이터를 복호화하는 데이터 복호화 장치

(100)이다.

[0031] 본 발명의 데이터 복호화 장치(100)는 통신부(110), 제1 연산부(120), 제2 연산부(130), 제3 연산부(140), 제4 연산부(150), 다항식 생성부(160) 및 판단부(170)를 포함한다.

[0032] 통신부(110)는 데이터가 암호화된 비트신호를 수신한다.

[0033] 제1 연산부(120)는 데이터의 암호화에 사용된 확산코드의 비트수에 대응하는 제1길이 만큼 비트신호에 비트 이동을 수행해 제1 연산스트림을 생성한다.

[0034] 여기서, 제1 연산부(120)는 왼쪽 시프트 연산을 수행하여 비트신호를 비트 이동시킨다.

[0035] 그리고, 제1 길이는 확산부호가 가질 수 있는 복수의 길이들 중 어느 하나이다.

[0036] 예를들어, 바커(Barker) 코드는 2, 3, 4, 5, 7, 11 및 13 비트로 생성될 수 있다.

[0037] 그러므로, 메시지를 암호화하는데 사용된 확산부호가 바커(Barker) 코드라면 제1 길이는 2, 3, 4, 5, 7, 11 및 13 중 어느 하나일 수 있다.

[0038] 제2 연산부(130)는 비트신호와 제1 연산스트림을 이용하여 확산부호가 상쇄된 제2 연산스트림을 생성한다.

[0039] 여기서, 제2 연산부(130)는 비트신호와 제1 연산스트림을 XOR 연산하여 데이터의 암호화에 사용된 확산부호를 상쇄한다.

[0040] 그리고, 제3 연산부(140)는 제2 연산스트림에 대하여 제2 길이만큼 비트 이동을 수행해 제3 연산스트림을 생성한다.

[0041] 여기서, 제3 연산부(140)는 왼쪽 시프트 연산을 수행하여 비트 이동을 할 수 있고, 제2 길이는 1 이상의 자연수일 수 있다.

[0042] 제4 연산부(150)는 제2 연산스트림과 제3 연산스트림을 이용하여 데이터가 상쇄된 제4 연산스트림을 생성한다.

[0043] 여기서, 제4 연산부(150)는 제2 연산스트림과 제3 연산스트림을 XOR 연산하여 데이터를 상쇄한다.

[0044] 다항식 생성부(160)는 제4 연산스트림을 이용하여 데이터를 복호화할 수 있는 생성다항식을 생성한다.

[0045] 다항식 생성부(160)는 제4 연산스트림을 생성다항식의 계수에 관한 선형 방정식으로 구성된 연립방정식으로 나타내고, 연립방정식을 행렬로 변환한 후 가우스 소거법을 적용하여 생성다항식의 계수를 추출한다.

[0046] 그리고, 추출된 계수를 이용하여 생성다항식을 생성한다.

[0047] 또한, 다항식 생성부(160)는 생성다항식을 생성함과 동시에 스크램블러의 초기값도 도출할 수 있다.

[0048] 판단부(170)는 생성다항식을 이용하여 비트신호를 복호화하고, 복호화 가능 여부를 판단한다.

[0049] 판단부(170)에서 비트신호가 생성다항식에 의해 복호화가 가능하면, 비트신호에 암호화된 데이터를 추출하고,

[0050] 비트신호가 복호화되지 않으면, 제1 연산부(120)에서 제1 연산스트림을 생성하는 과정부터 다시 반복하여 수행한다.

[0051] 여기서, 제1 연산부(120)는 확산부호의 다른 비트수로 제1 연산스트림을 생성한다.

[0052] 그리고, 제어부(180)는 데이터 복호화 장치(100)의 전반적인 동작을 제어한다.

[0054] 도 2는 본 발명의 일 실시예에 따른 데이터 복호화 방법을 설명하기 위한 흐름도이다.

[0055] 도 1 및 도 2를 참조하면, 본 발명의 데이터 복호화 방법은, 통신부(110)에서 데이터가 암호화된 비트신호를 수신한다(단계 S110).

[0056] 그리고, 제1 연산부(120)가 데이터의 암호화에 사용된 확산코드의 비트수에 대응하는 제1길이 만큼 비트신호에 대한 비트 이동을 수행하여 제1 연산스트림을 생성한다(단계 S120).

[0057] 단계 S120에서, 비트 이동은 왼쪽 시프트 연산으로 수행되고, 제1 길이는 확산부호가 가질 수 있는 복수의 비트수들 중 어느 하나이다.

[0058] 예를들어, 대표적인 확산부호인 바커(Barker) 코드는 2, 3, 4, 5, 7, 11 및 13비트의 길이로 생성될 수 있다.

[0059] 메시지를 암호화하는데 사용된 확산부호가 바커(Barker) 코드라면, 제1 길이는 2, 3, 4, 5, 7, 11 및 13 중 어느 하나일 수 있다.

[0060] 이후, 제2 연산부(130)가 비트신호와 제1 연산스트림을 이용하여 확산부호가 상쇄된 제2 연산스트림을 생성하고(단계 S130), 제3 연산부(140)가 제2 연산스트림에 제2 길이만큼 비트 이동을 수행해 제3 연산스트림을 생성한다(단계 S140).

[0061] 단계 S130에서, 제2 연산스트림은 비트신호와 제1 연산스트림 간의 배타적 논리합(Exclusive OR) 연산으로 생성되고, 이 과정에서 확산부호가 상쇄된다.

[0062] 단계 S140에서, 비트 이동은 왼쪽 시프트 연산으로 수행되고, 제2 길이는 1 이상의 자연수일 수 있다.

[0063] 그리고, 제4 연산부(150)가 제2 연산스트림과 제3 연산스트림을 이용하여 데이터가 상쇄된 제4 연산스트림을 생성하면(단계 S150), 다항식 생성부(160)가 제4 연산스트림을 이용하여 암호화된 데이터를 복호화할 수 있는 생성다항식을 생성한다(단계 S160).

[0064] 단계 S150에서, 제4 연산스트림은 제2 연산스트림과 제3 연산스트림 간의 배타적 논리합(Exclusive OR) 연산으로 생성되고, 이 과정에서 데이터가 상쇄된다.

[0065] 추가적으로, 단계 S160에서, 스크램블러의 초기값도 추출될 수 있다.

[0066] 이후, 판단부(170)가 단계 S160에서 생성된 생성다항식을 이용하여 비트신호를 복호화하고, 복호화 가능 여부를 판단한다(단계 S170).

[0067] 단계 S170에서, 생성다항식을 통해 비트신호의 복호화가 가능한 것으로 판단되면, 비트신호에 포함된 데이터를 복구하고,

[0068] 생성다항식을 통해 비트신호의 복호화가 불가능한 것으로 판단되면, 단계 S120으로 되돌아가 확산부호의 다른 비트수로 단계 S120, S130, S140, S150 및 S160을 재수행한다.

[0070] 도 3은 자기 동기 스크램블러의 구조를 나타낸 블록도이다.

[0071] 도 3을 참조하여 자기 동기 스크램블러로 암호화된 비트신호의 생성다항식을 도출하는 과정을 수식화하여 설명한다.

[0072] 자기 동기 스크램블러는 데이터가 LFSR(Linear Feedback Shift Register)로 입력되는 구조로 N 단의 자기 동기 스크램블러에서 i번째 스크램블링된 데이터가 생성될 때 LFSR 의 레지스터에는 이전 N 개의 값이 저장되어 있다.

[0073] 자기 동기 스크램블러의 생성다항식을 추정하는 것은 LFSR의 생성다항식 계수 $C=(C_1C_2\cdots C_N)$를 추정하는 것이다.

[0074] 여기에서, S는 통신부(110)에서 수신된 비트신호를 의미하고, $S=(S_1S_2\cdots)$ 로 나타낼 수 있다.

[0075] 그리고, 이를 이용하여 [수학식 1]을 도출할 수 있다.

*수학식 1*

$$s_i = m_i \oplus D_i$$

$$D_i = C \bullet (s_{i-1}s_{i-2}\cdots s_{i-N}) = [(c_1s_{i-1}) \oplus (c_2s_{i-2}) \oplus \cdots \oplus (c_Ns_N)]$$

[0076]

[0077] 여기서, $m_i$는 확산부호에 의해 변조된 데이터를 의미하고, $D_i$는 생성다항식을 의미하며, N은 LFSR의 생성다항식(generator polynomial)의 차수를 의미한다.

[0078] 그리고, [수학식 1]을 행렬로 변환하면, [수학식 2]로 나타낼 수 있다.

*수학식 2*

$$\begin{bmatrix} s_{i-1} & s_{i-2} & \cdots & s_{i-N} \\ s_i & s_{i-1} & \cdots & s_{i-N+1} \\ \vdots & \vdots & \ddots & \vdots \\ s_{i+N-2} & s_{i+N-3} & \cdots & s_{i-1} \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_N \end{bmatrix} + \begin{bmatrix} m_i \\ m_{i+1} \\ \vdots \\ m_{i+N-1} \end{bmatrix} = \begin{bmatrix} s_i \\ s_{i+1} \\ \vdots \\ s_{i+N-1} \end{bmatrix}$$

$$\begin{bmatrix} s_{i-1} & s_{i-2} & \cdots & s_{i-N} \\ s_i & s_{i-1} & \cdots & s_{i-N+1} \\ \vdots & \vdots & \ddots & \vdots \\ s_{i+N-2} & s_{i+N-3} & \cdots & s_{i-1} \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_N \end{bmatrix} = \begin{bmatrix} D_i \\ D_{i+1} \\ \vdots \\ D_{i+N-1} \end{bmatrix}$$

[0079]

[0080] 이후, 제1 연산부(120)에서 비트신호(S)에 확산부호의 비트 수만큼 왼쪽 시프트 연산을 수행하여 제1 연산스트림(S≪B)을 생성한다.

[0081] 여기서, B는 확산부호의 길이이다.

[0082] 그리고, 제2 연산부(130)가 비트신호와 제1연산스트림(S≪B) 간의 XOR 연산($S \oplus (S \ll B)$)으로 확산부호를 상쇄시켜 제2 연산스트림(T)를 생성한다.

[0083] 제2 연산스트림($T=t_0t_1t_2\cdots$)은 [수학식 3]과 같이 나타낼 수 있다.

*수학식 3*

$$\begin{aligned} T &= t_0\ t_1\ t_2\ \cdots \\ &= (s_0 \oplus s_B) \| (s_1 \oplus s_{B+1}) \| (s_2 \oplus s_{B+2}) \| (s_3 \oplus s_{B+3}) \| \cdots \\ &= (m_0 \oplus m_B \oplus D_0 \oplus D_B) \| (m_1 \oplus m_{B+1} \oplus D_1 \oplus D_{B+1}) \| (m_2 \oplus m_{B+2} \oplus D_2 \oplus D_{B+2}) \| \cdots \end{aligned}$$

[0084]

[0085] 이후, 제3 연산부(140)가 제2 연산스트림(T)에 1만큼 왼쪽 시프트 연산을 수행하여 제3 연산스트림(T≪1)을 생성한다.

[0086] 제3 연산스트림(T≪1)을 생성하는 과정에서 1만큼 비트 이동을 수행하였지만, 이에 한정되는 것은 아니며 사용자의 설정에 따라 다를 수 있다.

[0087] 그리고, 제4 연산부(150)에서 제2 연산스트림(T)과 제3 연산스트림(T≪1)간의 XOR 연산($T \oplus (T \ll 1)$)으로 데이터를 상쇄시켜 제4 연산스트림($U=u_0u_1u_2\cdots$)을 생성하고, 이를 [수학식 4]로 나타낼 수 있다.

*수학식 4*

$$u_i = \begin{cases} D_i \oplus D_{B+i} \oplus D_{i+1} \oplus D_{B+i+1} & \text{if } i \bmod B < B-1 \\ m_i \oplus m_{B+i} \oplus m_{i+1} \oplus m_{B+i+1} \oplus D_i \oplus D_{B+i} \oplus D_{i+1} \oplus D_{B+i+1} & else \end{cases}$$

[0088]

[0089] [수학식 4]에서 i mod B < B-1인 경우, $m_i \oplus m_{B+i} \oplus m_{i+1} \oplus m_{B+i+1}$ 에서 확산부호와 메시지는 상쇄된다.

[0090] 따라서, 각B개의 비트열마다 마지막 비트를 제외한 나머지 부분에서 $u_i$는 메시지와 확산부호가 모두 상쇄되어 $D_i$

들로만으로 구성된다.

[0091] 그리고, [수학식 1]의 $D_i=C\cdot(S_{i-1}S_{i-2}\cdots S_{i-n})$을 [수학식 4]의 $i \bmod B < B-1$인 경우에 대입하여 [수학식 5]를 도출할 수 있다.

*수학식 5*

[0092]
$$\begin{aligned} u_i &= c_1(s_{2i-1-N} \oplus s_{2i-N} \oplus s_{2i+1-N} \oplus s_{2i+2-N}) \\ &\quad \oplus c_2(s_{2i-N} \oplus s_{2i+1-N} \oplus s_{2i+2-N} \oplus s_{2i+3-N}) \oplus \cdots \oplus c_N(s_{2i-2} \oplus s_{2i-1} \oplus s_{2i} \oplus s_{2i+1}) \\ &= \bigoplus_{j=1}^{N} c_j u_{i-j} \text{ for } i \bmod B < B-1. \end{aligned}$$

[0093] 이후, 다항식 생성부(160)에서 [수학식 5]를 이용하여 $u_i$들을 $C=(C_1C_2\cdots C_N)$에 관한 선형 방정식으로 구성된 연립방정식으로 나타내고, 행렬로 변환하여 가우스 소거법을 적용해 C의 값을 구한다.

[0094] 그리고, 구해진 C 값을 이용하여 생성다항식을 도출하고, 스크램블러의 초기값을 구할 수 있다.

[0095] 이후, 판단부(170)가 도출된 생성다항식을 이용하여 비트신호를 복호화하는데, 비트신호가 생성다항식에 의해 복호화되는 것으로 판단되면 비트신호에 포함된 데이터를 추출하고,

[0096] 비트신호가 복호화되지 않는 것으로 판단되면, 확산부호의 다른 비트수로 제1 연산스트림을 생성하는 과정부터 다시 수행하게 된다.

[0098] 데이터가 암호화된 미상의 비트신호를 수신하면, 암호화에 사용된 확산부호의 길이를 모르는 경우가 많기 때문에, 길이를 모른다는 가정하에 예를 들어 생성다항식을 구하는 과정을 설명한다.

[0099] 먼저, 확산부호로 Walsh 코드가 사용된 경우를 설명한다.

[0100] 비트신호를 수신하면 Walsh 코드의 길이를 모르기 때문에, 모든 Walsh 코드의 길이에 대해 본 발명을 수행하여야 한다.

[0101] 그러나, Walsh의 특성상 Walsh 코드는 $2^m$의 길이를 가지므로, 길이가 $2^m$인 Walsh 코드로 확산된 비트신호(S)가 주어졌을 때, 언제나 2의 배수 단위의 비트 이동을 하므로 2가 최소 비트 이동의 단위가 되어 제1 연산스트림은 $S\ll 2^m$ 연산으로 생성될 수 있다.

[0102] 따라서, 제2 연산스트림(T)은 $S \oplus (S \ll 2)$ 연산으로 생성될 수 있고, Walsh 코드의 길이에 상관없이 생성다항식과 초기값을 계산할 수 있다.

[0103] 또한, 확산부호로 Barker 코드가 사용된 경우를 설명하면,

[0104] 마찬가지로, 미상의 비트신호를 수신하면 사용된 Barker 코드의 길이를 모르기 때문에 모든 Barker 코드의 길이에 대해 적용하여야 한다.

[0105] 그런데, Barker 코드는 길이가 2, 3, 4, 5, 7, 11 및 13으로 7가지이므로, 7번만 수행하면 된다.

[0106] 그리고, 2는 4의 약수이기 때문에, 길이가 2인 바커(Barker) 코드의 경우 4와 동일한 생성다항식과 초기값을 얻을 수 있으므로 길이 3, 4, 5, 7, 11 및 13에 대해서 최대 6번 적용하면 생성다항식을 생성할 수 있다.

[0107] 이렇게, 미상의 비트신호에 확산부호로 Walsh코드와 Barker코드를 사용되었다는 것을 안다는 전제하에 예를들어 설명하였지만 이에 한정되는 것은 아니며, 확산부호를 몰라도 확산부호의 특징을 적용하여 본 발명을 반복수행하여 생성다항식을 도출할 수 있다.

[0108] 추가적으로, 암호화에 사용된 확산부호의 종류를 몰라도 어느 하나의 확산부호로 가정한 후, 확산부호가 가질 수 있는 길이의 특성을 적용하여 생성다항식을 도출할 수 있다.

[0110] 이상 실시예를 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허 청구의 범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을

이해할 수 있을 것이다.

## 부호의 설명

[0111] 110...통신부 120...제1 연산부

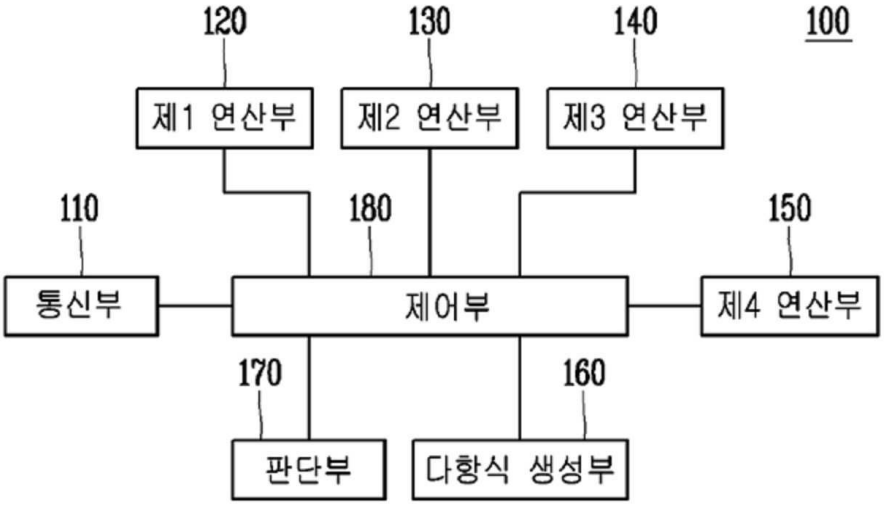
130...제2 연산부 140...제3 연산부

150...제4 연산부 160...다항식 생성부

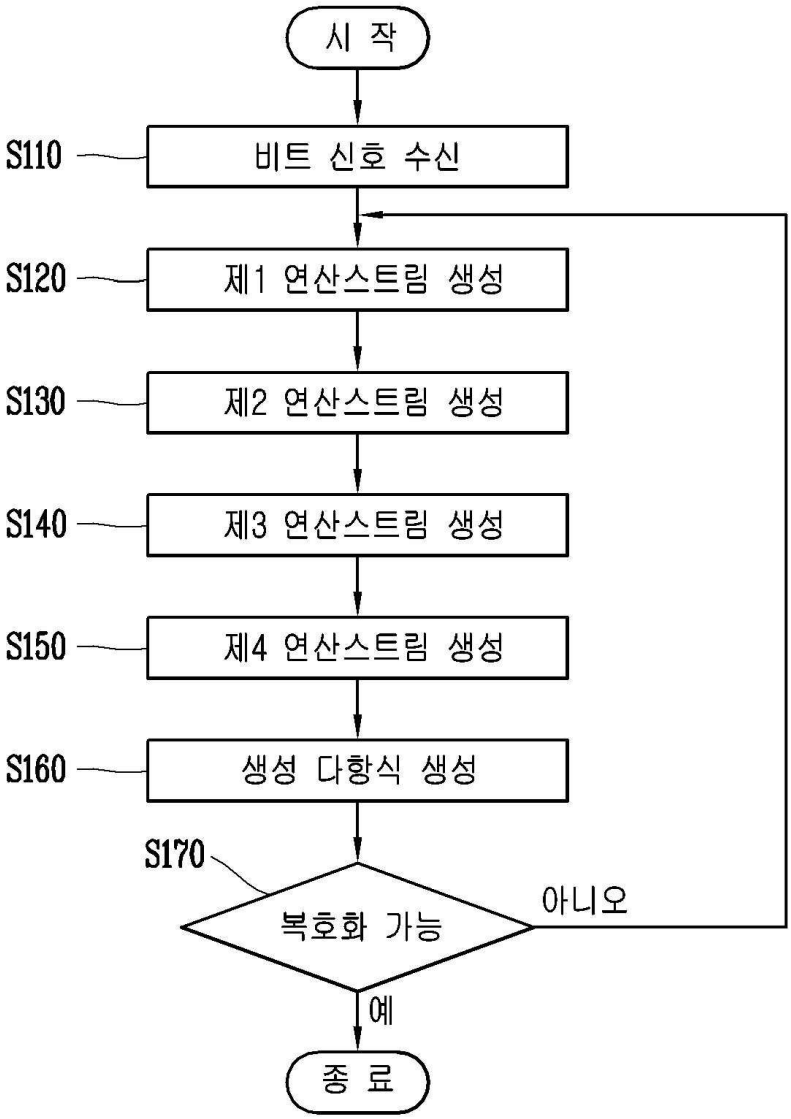
170...판단부 180...제어부

## 도면

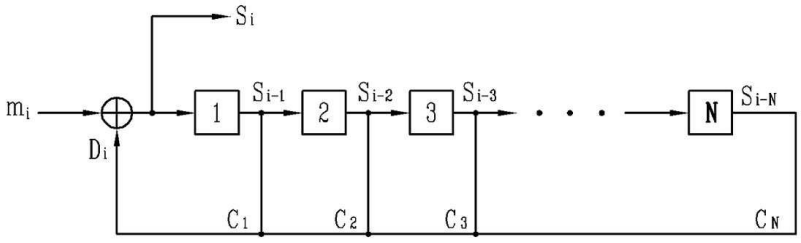
### 도면1



도면2


시 작
S110
비트 신호 수신
S120
제1 연산스트림 생성
S130
제2 연산스트림 생성
S140
제3 연산스트림 생성
S150
제4 연산스트림 생성
S160
생성 다항식 생성
S170
복호화 가능
아니오
예
종 료

도면3


Si
mi
Di
1
2
3
N
Si-1
Si-2
Si-3
Si-N
C1
C2
C3
CN