



(19) 대한민국특허청(KR)  
(12) 공개특허공보(A)

(11) 공개번호 10-2012-0068999  
(43) 공개일자 2012년06월28일

(51) 국제특허분류(Int. Cl.)

H01J 13/10 (2006.01) H04B 1/69 (2011.01)

(21) 출원번호 10-2010-0106126

(22) 출원일자 2010년10월28일

심사청구일자 2010년10월28일

(71) 출원인

서강대학교산학협력단

서울특별시 마포구 백범로 35 (신수동, 서강대학교)

(72) 발명자

김대산

서울특별시 강서구 양천로71길 38, 월드메르디앙 아파트 105-902 (염창동)

(74) 대리인

특허법인충현

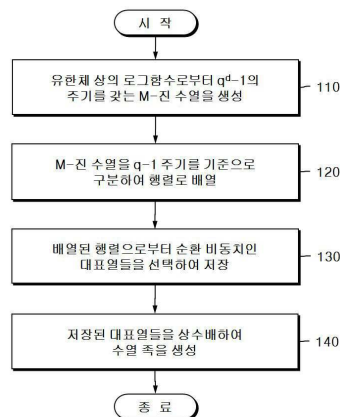
전체 청구항 수 : 총 17 항

(54) 발명의 명칭 통신 시스템의 채널 확산을 위한 수열 족의 생성 장치 및 방법

### (57) 요약

본 발명은 통신 시스템의 채널 확산을 위한 수열 족의 생성 장치 및 방법에 관한 것으로, 본 발명에 따른 통신 시스템의 채널 확산을 위한 수열 족을 생성하는 방법은 유한체 상의 로그함수를 이용하여  $q^d-1$  ( $q$ 는 소수승,  $d$ 는 2 이상인 정수)의 주기를 갖는  $M$ -진( $M$ 은  $q-1$ 의 약수) 수열을  $q-1$  주기를 기준으로 구분하여 행렬로 배열하고, 배열된 행렬로부터 순환 비동치인 대표열들을 선택하여 저장하고, 저장된 대표열들을 상수배함으로써 수열 족을 생성한다.

### 대표도 - 도1



## 특허청구의 범위

### 청구항 1

통신 시스템의 채널 확산을 위한 수열 족(sequence family)을 생성하는 방법에 있어서,

유한체 상의 로그함수를 이용하여  $q^d-1$ ( $q$ 는 소수승,  $d$ 는 2 이상인 정수)의 주기를 갖는  $M$ -진( $M$ 은  $q-1$ 의 약수) 수열을 생성하는 단계;

상기  $M$ -진 수열을  $q-1$  주기를 기준으로 구분하여 행렬로 배열하는 단계;

상기 배열된 행렬로부터 순환 비동치(cyclically inequivalent/distinct)인 대표열들을 선택하여 저장하는 단계; 및

상기 저장된 대표열들을 상수배하여 수열 족을 생성하는 단계를 포함하고,

상기 수열 족의 점근적 크기는 상기  $q$ 의 정수승에 비례하는 것을 특징으로 하는 방법.

### 청구항 2

제 1 항에 있어서,

상기 순환 비동치인 대표열은  $q$ -원분 잉여류( $q$ -cyclotomic coset)의 최소 정수인 것을 특징으로 하는 방법.

### 청구항 3

제 1 항에 있어서,

상기  $M$ -진 수열은  $M$ -진 시델니코프(Sidel'nikov) 수열인 것을 특징으로 하는 방법.

### 청구항 4

제 1 항에 있어서,

상기 생성된 수열 족의 최대상관수(maximum correlation magnitude)는  $(2d-1)\sqrt{q}+1$  ( $d$ 는 1보다 큰 양의 정수)를 상계로 갖는 것을 특징으로 하는 방법.

### 청구항 5

제 1 항에 있어서,

상기 점근적 크기는  $\frac{(M-1)q^{d-1}}{d}$  ( $d$ 는 1보다 큰 양의 정수)인 것을 특징으로 하는 방법.

### 청구항 6

제 1 항에 있어서,

상기 행렬은 상기  $M$ -진 수열을  $(q-1) \times \left(\frac{q^d-1}{q-1}\right)$  ( $d$ 는 1보다 큰 양의 정수)의 형태로 배열한 것을 특징으로 하는 방법.

### 청구항 7

제 1 항 내지 제 6 항 중에 어느 한 항의 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

### 청구항 8

통신 시스템의 채널 확산을 위한 수열 족을 생성하는 장치에 있어서,

유한체 상의 로그함수를 이용하여  $q^d-1$ ( $q$ 는 소수승,  $d$ 는 2 이상인 정수)의 주기를 갖는  $M$ -진( $M$ 은  $q-1$ 의 약수) 수열을 생성하는 수열 생성부;

상기  $M$ -진 수열을  $q-1$  주기를 기준으로 구분하여 행렬로 배열하고, 상기 배열된 행렬으로부터 순환 비동치인 대표열들을 선택하는 연산부;

상기 배열된 행렬과 선택된 대표열들을 저장하는 저장부; 및

상기 저장된 대표열들을 상수배하여 수열 족을 생성하는 수열 족 생성부를 포함하고,

상기 수열 족의 점근적 크기는 상기  $q$ 의 정수승에 비례하는 것을 특징으로 하는 장치.

#### 청구항 9

제 8 항에 있어서,

상기  $M$ -진 수열은  $M$ -진 시텔니코프 수열이고,

상기 순환 비동치인 대표열은  $q$ -원분 잉여류의 최소 정수인 것을 특징으로 하는 장치.

#### 청구항 10

제 8 항에 있어서,

상기 생성된 수열 족의 최대상관수는  $(2d-1)\sqrt{q}+1$  ( $d$ 는 1보다 큰 양의 정수)를 상계로 갖고,

상기 점근적 크기는  $\frac{(M-1)q^{d-1}}{d}$  ( $d$ 는 1보다 큰 양의 정수)인 것을 특징으로 하는 장치.

#### 청구항 11

제 8 항에 있어서,

상기 행렬은 상기  $M$ -진 수열을  $(q-1) \times \left(\frac{q^d-1}{q-1}\right)$  ( $d$ 는 1보다 큰 양의 정수)의 형태로 배열한 것을 특징으로 하는 장치.

#### 청구항 12

통신 시스템의 채널 확산을 위한 확산(spreading) 신호의 생성 장치에 있어서,

디지털 변조된 신호를 입력받는 입력부;

소정 수열 족으로부터 확산 코드(code)를 생성하는 확산 코드 생성부; 및

상기 입력된 신호에 상기 생성된 확산 코드를 승산하여 대역폭을 확산시킴으로써 확산 신호를 생성하는 확산 신호 생성부를 포함하고,

상기 소정 수열 족은 유한체 상의 로그함수를 이용하여  $q^d-1$ ( $q$ 는 소수승,  $d$ 는 2 이상인 정수)의 주기를 갖는  $M$ -진( $M$ 은  $q-1$ 의 약수) 수열을 생성하고, 상기  $M$ -진 수열을  $q-1$  주기를 기준으로 구분하여 행렬로 배열하고, 상기 배열된 행렬으로부터 순환 비동치인 대표열들을 선택하여 저장하고, 상기 저장된 대표열들을 상수배함으로써 생성되며,

상기 수열 족의 점근적 크기는 상기  $q$ 의 정수승에 비례하는 것을 특징으로 하는 장치.

#### 청구항 13

제 12 항에 있어서,

상기  $M$ -진 수열은  $M$ -진 시텔니코프 수열이고,

상기 순환 비동치인 대표열은  $q$ -원분 잉여류의 최소 정수인 것을 특징으로 하는 장치.

#### 청구항 14

제 12 항에 있어서,

상기 행렬은 상기 M-진 수열을  $(q-1) \times \left(\frac{q^d-1}{q-1}\right)$  (d는 1보다 큰 양의 정수)의 형태로 배열한 것을 특징으로 하는 장치.

#### 청구항 15

통신 시스템의 채널 확산을 위한 확산 신호를 역확산(despreading)하는 장치에 있어서,

확산(spreading) 신호를 수신하는 수신부;

소정 수열 족으로부터 확산 코드를 생성하는 확산 코드 생성부; 및

상기 수신된 확산 신호에 상기 생성된 확산 코드를 승산하여 대역폭을 역확산시킴으로써 확산 신호의 원본 신호를 복원하는 신호 복원부를 포함하고,

상기 소정 수열 족은 유한체 상의 로그함수를 이용하여  $q^d-1$ (q는 소수승, d는 2 이상인 정수)의 주기를 갖는 M-진(M은 q-1의 약수) 수열을 생성하고, 상기 M-진 수열을 q-1 주기를 기준으로 구분하여 행렬로 배열하고, 상기 배열된 행렬으로부터 순환 비동치인 대표열들을 선택하여 저장하고, 상기 저장된 대표열들을 상수배함으로써 생성되며,

상기 수열 족의 점근적 크기는 상기 q의 정수승에 비례하는 것을 특징으로 하는 장치.

#### 청구항 16

제 15 항에 있어서,

상기 M-진 수열은 M-진 시탈니코프 수열이고,

상기 순환 비동치인 대표열은 q-원분 잉여류의 최소 정수인 것을 특징으로 하는 장치.

#### 청구항 17

제 15 항에 있어서,

상기 행렬은 상기 M-진 수열을  $(q-1) \times \left(\frac{q^d-1}{q-1}\right)$  (d는 1보다 큰 양의 정수)의 형태로 배열한 것을 특징으로 하는 장치.

### 명세서

#### 기술분야

[0001] 본 발명은 통신 시스템의 채널 확산을 위한 수열 족의 생성 장치 및 방법에 관한 것으로, 특히 코드분할 다중 접속(code-division multiple-access, CDMA) 통신 시스템과 같은 대역 확산(spread-spectrum) 기술을 사용하는 통신 환경 하에서 확산 코드(spreading code)에 활용되는 수열 족(sequence family)을 생성하는 장치, 방법 및 이를 기록한 기록매체에 관한 것이다.

#### 배경기술

[0002] CDMA 통신 시스템은 대역 확산 기술을 활용하여 전체 대역 내에서 각각의 정보를 측정 부호 및 시간 차이로 분할하여 보내고 수신측에서도 전체 대역 내의 많은 정보들 중 송신시 사용된 것과 동일한 부호와 시간 차이를 갖는 정보만을 선택하여 원본 신호를 복원하는 통신 방식을 말한다. 이러한 CDMA는 모든 서비스 영역에서 동일한 주파수를 다수의 셀(cell)에서 사용할 수 있기 때문에 주파수 이용 효율이 타 방식에 비해서 월등히 높으며, 서로 다른 코드를 사용하여 통신을 하기 때문에 무선 구간의 통신 비밀 보호 특성이 매우 우수하다는 특징이 있다.

[0003] 특히, 대역 확산(이하에서는 대역 확산 또는 채널 확산의 용어로서 사용될 것이다.) 기술은 특정한 정보를 전송하기 위해 필요한 이론적 대역폭보다 훨씬 넓은 대역폭을 사용하여 정보를 전송하는 기법으로서, 우수한 오류 효율 또는 신호 대 잡음비를 갖는다. 또한 확산되어 송신되는 신호의 세기가 매우 약하더라도 통신이 가능하고 잡음 신호에 강하기 때문에 많은 송신자가 동시에 신호를 송출하더라도 특정 코드를 가진 특정 수신자에게 신호를 전달할 수 있다. 즉, 하나의 채널을 여러 사용자가 동시에 사용할 수 있으므로 그만큼 용량이 증대될 수 있다. 대역 확산 기법에는 직접 시퀀스(DS:direct sequence) 기법, 주파수 도약(FH:frequency hopping) 기법, 시간 도약(TH:time hopping) 기법, 칩 대역 확산 기법 등이 알려져 있으며, 이들 중 2가지를 혼합 사용하는 혼성 방식도 많이 이용된다.

[0004] 이러한 대역 확산 기술에 기반한 고속 데이터 통신의 수요가 증가면서 좋은 상관 특성을 갖는 수열을 찾는 것이 점점 더 중요해지고 있다. 이러한 수열은 무선 통신의 대역 확산 시스템에서 다중 접속 코드로 이용하기 위해 높은 보안성을 보장하면서도 다수의 송신자가 동시에 신호를 송출할 수 있도록 선형복잡도가 크면서도 수열 족의 크기가 클 것을 요구한다.

## 발명의 내용

### 해결하려는 과제

[0005] 본 발명이 해결하고자 하는 기술적 과제는 채널 확산 기술을 사용하는 통신 시스템의 수요 증가에 따라 하나의 채널에 포함될 수 있는 송신 데이터의 수가 포화에 이르게 될 한계를 극복하고, 불법적인 무선 통신 감청이나 해킹의 우려를 해소할 수 있으며, 나아가 스트림 암호 시스템 및 차세대 이동 통신 시스템에서 요구하는 강력한 보안과 안정성을 가진 수열 족을 제공하는데 있다.

### 과제의 해결 수단

[0006] 상기 기술적 과제를 해결하기 위하여, 본 발명에 따른 통신 시스템의 채널 확산을 위한 수열 족을 생성하는 방법은 유한체 상의 로그함수를 이용하여  $q^d-1$ ( $q$ 는 소수승,  $d$ 는 2 이상인 정수)의 주기를 갖는  $M$ -진( $M$ 은  $q-1$ 의 약수) 수열을 생성하는 단계; 상기  $M$ -진 수열을  $q-1$  주기를 기준으로 구분하여 행렬로 배열하는 단계; 상기 배열된 행렬로부터 순환 비동치인 대표열들을 선택하여 저장하는 단계; 및 상기 저장된 대표열들을 상수배하여 수열 족을 생성하는 단계를 포함하고, 상기 수열 족의 점근적 크기는 상기  $q$ 의 정수승에 비례한다.

[0007] 또한, 이하에서는 상기 기재된 통신 시스템의 채널 확산을 위한 수열 족을 생성하는 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공한다.

[0008] 상기 기술적 과제를 해결하기 위하여, 본 발명에 따른 통신 시스템의 채널 확산을 위한 수열 족을 생성하는 장치는 유한체 상의 로그함수를 이용하여  $q^d-1$ ( $q$ 는 소수승,  $d$ 는 2 이상인 정수)의 주기를 갖는  $M$ -진( $M$ 은  $q-1$ 의 약수) 수열을 생성하는 수열 생성부; 상기  $M$ -진 수열을  $q-1$  주기를 기준으로 구분하여 행렬로 배열하고, 상기 배열된 행렬로부터 순환 비동치인 대표열들을 선택하는 연산부; 상기 배열된 행렬과 선택된 대표열들을 저장하는 저장부; 및 상기 저장된 대표열들을 상수배하여 수열 족을 생성하는 수열 족 생성부를 포함하고, 상기 수열 족의 점근적 크기는 상기  $q$ 의 정수승에 비례한다.

[0009] 상기 기술적 과제를 해결하기 위하여, 본 발명에 따른 통신 시스템의 채널 확산을 위한 수열 족을 생성하는 장치, 방법 및 기록매체에서 상기  $M$ -진 수열은  $M$ -진 시델니코프 수열이고, 상기 순환 비동치인 대표열은  $q$ -원 분 잉여류의 최소 정수인 것이 바람직하다.

[0010] 상기 다른 기술적 과제를 해결하기 위하여, 본 발명에 따른 통신 시스템의 채널 확산을 위한 확산 신호의 생성 장치는 디지털 변조된 신호를 입력받는 입력부; 소정 수열 족으로부터 확산 코드를 생성하는 확산 코드 생성부; 및 상기 입력된 신호에 상기 생성된 확산 코드를 승산하여 대역폭을 확산시킴으로써 확산 신호를 생성하는 확산 신호 생성부를 포함하고, 상기 소정 수열 족은 유한체 상의 로그함수를 이용하여  $q^d-1$ ( $q$ 는 소수승,  $d$ 는 2 이상인 정수)의 주기를 갖는  $M$ -진( $M$ 은  $q-1$ 의 약수) 수열을 생성하고, 상기  $M$ -진 수열을  $q-1$  주기를 기준으로 구분하여 행렬로 배열하고, 상기 배열된 행렬로부터 순환 비동치인 대표열들을 선택하여 저장하고, 상기 저장된 대표열들을 상수배함으로써 생성되며, 상기 수열 족의 점근적 크기는 상기  $q$ 의 정수승에 비례한다.

[0011] 상기 다른 기술적 과제를 해결하기 위하여, 본 발명에 따른 통신 시스템의 채널 확산을 위한 확산 신호를 역

확산하는 장치는 확산 신호를 수신하는 수신부; 소정 수열 족으로부터 확산 코드를 생성하는 확산 코드 생성부; 및 상기 수신된 확산 신호에 상기 생성된 확산 코드를 승산하여 대역폭을 역확산시킴으로써 확산 신호의 원본 신호를 복원하는 신호 복원부를 포함하고, 상기 소정 수열 족은 유한체 상의 로그함수를 이용하여  $q^d - 1$  ( $q$ 는 소수승,  $d$ 는 2 이상인 정수)의 주기를 갖는  $M$ -진( $M$ 은  $q-1$ 의 약수) 수열을 생성하고, 상기  $M$ -진 수열을  $q-1$  주기를 기준으로 구분하여 행렬로 배열하고, 상기 배열된 행렬으로부터 순환 비동치인 대표열들을 선택하여 저장하고, 상기 저장된 대표열들을 상수배함으로써 생성되며, 상기 수열 족의 점근적 크기는 상기  $q$ 의 정수승에 비례한다.

[0012] 상기 다른 기술적 과제를 해결하기 위하여, 본 발명에 따른 통신 시스템의 채널 확산을 위한 확산 신호의 생성 장치 및 확산 신호를 역확산하는 장치에서 상기  $M$ -진 수열은  $M$ -진 시델니코프 수열이고, 상기 순환 비동치인 대표열은  $q$ -원분 잉여류의 최소 정수인 것이 바람직하다.

### 발명의 효과

[0013] 본 발명은 채널 확산 기술을 사용하는 통신 시스템의 폭발적인 수요 증가에 부응하여 하나의 채널에 포함될 수 있는 송신 데이터의 수를 비약적으로 증가시킴으로써 채널 내 데이터 포화의 한계를 극복하고, 낮은 상관성질로 인해 불법적인 무선 통신 감청이나 해킹에 강인한 특성을 갖는 수열 족을 제공함으로써 스트림 암호 시스템 및 차세대 이동 통신 시스템에서 요구하는 강력한 보안과 안정성을 보장할 수 있다.

### 도면의 간단한 설명

[0014] 도 1은 본 발명의 일 실시예에 따른 통신 시스템의 채널 확산을 위한 수열 족을 생성하는 방법을 도시한 흐름도이다.

도 2는 본 발명의 일 실시예에 따른 통신 시스템의 채널 확산을 위한 수열 족을 생성하는 장치를 도시한 블록도이다.

도 3은 본 발명의 다른 실시예에 따른 통신 시스템의 채널 확산을 위한 일련의 통신 과정을 설명하기 위한 도면이다.

도 4a 및 도 4b는 각각 본 발명의 다른 실시예에 따른 통신 시스템의 채널 확산을 위한 확산 신호의 생성 장치 및 확산 신호를 역확산하는 장치를 도시한 도면이다.

도 5는 종래에 알려진 방법에 의해 생성된 수열 족들의 특성을 비교하여 설명하기 위한 도면이다.

### 발명을 실시하기 위한 구체적인 내용

[0015] 본 발명의 실시예들을 구체적으로 설명하기에 앞서, 본 발명의 실시예들이 구현될 수 있는 대표적인 환경인 대역 확산 통신 방식에 대해 개괄적으로 소개하고자 한다.

[0016] 일반적인 디지털 통신에서는 송신하고자 하는 데이터를 PSK(phase shift keying)나 FSK(frequency shift keying) 방식으로 디지털 변조하여 송신한다. 어떠한 정보를 전송할 때에는 그 정보를 전송하기 위해 이론적으로 필요한 주파수 대역폭을 산출하게 되고, 산출 결과에 의해 해당 정보를 전송하기 위한 주파수의 대역폭이 결정된다.

[0017] 그러나, 확산 대역(spread spectrum) 통신에서는 이론적으로 산출된 필요 주파수 대역폭보다 훨씬 넓은 대역폭을 사용하여 정보를 전송한다. 예를 들어, 음성은 최대 4KHz의 주파수 대역을 가지므로 기술적으로는 최소 4KHz의 대역폭만 있으면 음성 신호의 전송이 가능하다. 그러나, CDMA와 같은 확산 대역 통신 방식에서는 이것보다 300배 이상 넓은 1.25MHz의 주파수 대역폭을 사용하여 음성 신호를 전송한다.

[0018] 구체적으로, 확산 대역 통신에서는 디지털 변조된 신호에 고속의 확산 코드를 승산하여 주파수의 대역폭을 광대역으로 확장시킨 후 확산된(spreading) 신호를 전송한다. 이어서 수신측에서는 송신측에서 사용한 것과 동일한 고속의 확산 코드를 승산함으로써 주파수의 대역폭을 협대역으로 변환하는 역확산(despreading) 과정을 거친 후 복조를 하게 된다. 일반적으로 무선 전송 과정에서는 잡음(noise)이 유입되게 되는데 이 때 유입된 잡음은 수신측에서 승산된 확산 코드에 의해 그 영향이 줄어들게 된다.

[0019] 간단한 수식을 통해 이를 설명하면 다음의 수학적 식 1과 같다.

## 수학식 1

$$\{(S \cdot C) + N\} \cdot C = (S \cdot C) \cdot C + N \cdot C = S + N \cdot C$$

[0020]

[0021]

수학식 1에서 S는 원신호를 의미하고, C는 확산 코드를 의미하며, N은 잡음을 의미한다. 확산 코드 통신 방식에서는 원신호에 확산코드를 승산하여 전송한다고 하였으므로 전송되는 신호는 S?C 가 될 것이다. 여기에 전송 과정에서 잡음이 유입되므로 수신측에 도착한 신호는 (S?C) + N 가 될 것이다. 이제 수신측에서는 원신호를 복원하기 위해 송신시에 사용하였던 확산 코드와 동일한 확산 코드를 다시 한 번 승산하므로 {(S?C) + N}?C 와 같이 표현될 수 있다. 여기서 확산 코드는 동일한 코드를 서로 승산하였을 때, 1이 되는 특징이 있음에 주목하자. 따라서, 상기 수학식 1과 같은 연산 결과 S + N?C 를 얻을 수 있다. 결과에서 볼 수 있듯이 원신호 S는 수신측에서 정상적으로 복원되는 반면, 잡음 N은 확산 코드 C가 승산되어 넓게 확산되므로 그 영향이 감소하게 된다.

[0022]

디지털 셀룰러 CDMA 방식에서 10KHz의 대역폭을 가진 신호를 1.25MHz의 대역폭을 갖도록 확산시키면 이 확산된 정보 신호는 넓은 주파수 대역에 골고루 퍼져서 그 신호의 세기가 원래의 신호에 비해서 희미해지게 된다. 그 결과, 이렇게 확산된 신호를 수신하려면 전체 주파수 대역을 모두 검색해 보아야 하므로 상대적으로 그 신호의 존재를 알기 어렵다고 볼 수 있다. 즉, 전송 신호가 희미해지므로 다른 신호에 간섭을 적게 주며, 보안의 신뢰도가 높아진다. 또한, 확산 신호가 넓은 주파수 대역에 걸쳐 퍼져 있으므로 전파 과정에서 간섭이나 잡음이 포함되더라도 넓은 주파수 대역 중 그 영향이 일부분에만 미치게 된다. 따라서, 간섭이나 잡음의 영향이 상당히 감소하므로 통화 품질이 향상될 수 있다.

[0023]

CDMA 통신 시스템에서는 동기화(synchronization) 및 다중 접속 간섭(interference)의 최소화를 위해 낮은 상관을 갖는 수열이 요구된다. 특히, 적응적 변조 방법(adaptive modulation schemes)에서는 채널 특징에 따른 데이터 비율을 최대화시키기 위해 가변적인 길이 및 알파벳 크기를 갖는 수열이 바람직하다. 나아가, 가능한 많은 사용자들을 지원하기 위해 다수의 식별되는(distinct) 수열이 필요하다.

[0024]

이하에서는 이러한 요구에 부응하는 새로운 수열 족을 제안하고, 도면을 참조하여 본 발명의 다양한 실시예들을 상세하게 설명한다. 이하의 실시예들 전반에 걸쳐 다음과 같은 기호를 사용하기로 한다. p는 소수(prime number)를 의미하고, n은 양의 정수를 의미하고, q는  $p^n$ 을 의미하고,  $\mathbb{F}_q$ 는 q개의 원을 갖는 유한체(finite field)를 의미하고,  $\mathbb{F}_{q^d}$ 는  $q^d$  ( $d \geq 2$ ) 개의 원을 갖는 유한체를 의미하고, M은  $M \geq 2$ 인  $q-1$ 의 양의 약수를 의미하고,  $w_M = \exp(\frac{2\pi i}{M})$ 이고,  $\alpha$ 는  $\mathbb{F}_{q^d}$ 의 한 원시원이고,  $\beta$ 는  $\beta = \alpha^{\frac{q^d-1}{N}} = N(\alpha)$ 인  $\mathbb{F}_q$ 의 한 원시원(primitive element)이고, N은  $N(x) = x^{\frac{q^d-1}{q-1}}$ 로 주어지는  $\mathbb{F}_{q^d}$ 에서  $\mathbb{F}_q$ 로의 노름 사상(norm map)이고, Tr은  $\text{Tr}(x) = \sum_{j=0}^{d-1} x^{q^j}$ 로 주어지는  $\mathbb{F}_{q^d}$ 에서  $\mathbb{F}_q$ 로의 트레이스 사상(trace map)이며,  $\psi$ 는  $\psi_{(x)} = \exp(\frac{2\pi i \log_{\beta} x}{M}) = w_M^{\log_{\beta} x}$ 로 주어지는 위수(order) M인  $\mathbb{F}_q$ 의 곱 지표(multiplicative character)를 의미한다. 이제  $\beta$ 를  $\mathbb{F}_q$ 의 임의의 한 원시원이라 하면,  $\mathbb{F}_q$ 상의 로그함수(logarithm)는 다음의 수학식 2와 같다.

## 수학식 2

$$\log_{\beta} x = \begin{cases} t, & \text{if } x = \beta^t \ (0 \leq t \leq q-2), \\ 0, & \text{if } x = 0. \end{cases}$$

[0025]

[0026] 이제  $\mathbb{F}_q$ 의 어떤 고정된 원시원  $\beta$ 에 대해 주기(period)가  $q-1$ 인  $M$ -진( $M$ -ary) 시델니코프(Sidelnikov) 수열(sequence)  $s(t)$ 는 다음의 수학적 식 3과 같이 정의된다.

### 수학적 식 3

$$s(t) = \begin{cases} k, & \text{if } \beta^t \in D_k, \\ 0, & \text{if } \beta^t = -1, \end{cases}$$

$$D_k = \{\beta^{Mj+k} - 1 | 0 \leq j < \frac{q-1}{M}\}, \text{ for } 0 \leq k \leq M-1$$

[0029] 그러면, 주기  $q-1$ 인  $M$ -진 시델니코프 수열  $s(t)$ 는 다음의 수학적 식 4과 같이 간략히 기술된다.

### 수학적 식 4

$$s(t) \equiv \log_{\beta}(\beta^t + 1) \pmod{M}$$

[0031] or

$$w_M^{s(t)} = \psi(\beta^t + 1)$$

[0033] 곱 지표 합(multiplicative character sums)에 대한 Weil의 추정(Weil's estimate)는 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에게 잘 알려져 있다.

[0034] 이어서 주기가  $q^d-1$ 인  $M$ -진 시델니코프 수열의 배열(array) 구조에 대해 살펴본다. 여기서 보다 강한 조건을 가정하여  $M$ 을  $q^d-1$ 의 약수가 아닌  $q-1$ 의 약수라고 하면, 주기가  $q^d-1$ 인  $M$ -진 시델니코프 수열은 다음의 수학적 식 5와 같다.

### 수학적 식 5

$$s(t) \equiv \log_{\beta}(N(\alpha^t + 1)) \pmod{M}$$

$$0 \leq t \leq q^d - 2$$

[0037] 수학적 식 5는 다음의 수학적 식 6과 같이 표현될 수도 있다.

### 수학적 식 6

$$s(t) = \begin{cases} 0, & \text{if } N(\alpha^t + 1) = 0, \\ k, & \text{if } N(\alpha^t + 1) \in S_k \end{cases}$$

$$S_k = \{\beta^{Mj+k} | 0 \leq j < \frac{q-1}{M}\} \text{ for } 0 \leq k \leq M-1$$

[0040] 이러한 수학적 식 5는 다음과 같이 시델니코프 수열의 정의로부터 유도될 수 있다.

### 수학식 7

$$s(t) \equiv y(t) \pmod{M}$$

$$y(t) = \log_{\alpha}(\alpha^t + 1)$$

수학식 5를 증명하기 위해  $N(\alpha^t + 1) \neq 0$  라고 가정하면,

### 수학식 8

$$N(\alpha^t + 1) = \beta^{x(t)}$$

$$\begin{aligned} \frac{q^d - 1}{q - 1} y(t) &\equiv \log_{\alpha}(\alpha^t + 1)^{\frac{q^d - 1}{q - 1}} \\ &\equiv \log_{\alpha} N(\alpha^t + 1) \\ &\equiv \log_{\alpha} \alpha^{\frac{q^d - 1}{q - 1} x(t)} \\ &\equiv \frac{q^d - 1}{q - 1} x(t) \pmod{q^d - 1} \end{aligned}$$

이상으로부터 다음의 수학식 9가 유도된다.

### 수학식 9

$$x(t) \equiv y(t) \pmod{q - 1}$$

따라서,  $M$ 이  $q-1$ 의 약수일 때,  $x(t) \equiv y(t) \pmod{M}$  이므로 다음의 수학식 10이 성립함을 알 수 있다.

### 수학식 10

$$s(t) \equiv y(t) \equiv x(t) \equiv \log_{\beta} N(\alpha^t + 1) \pmod{M}$$

이제 수학식 5의 주기가  $q^d - 1$ 인  $M$ -진 시퀀스 코프 수열  $\{s(t)\}$  ( $0 \leq t \leq q^d - 2$ ) 을  $(q - 1) \times (\frac{q^d - 1}{q - 1})$  의 행렬로 배열한다. 이렇게 배열된 행렬의 1-번째 열  $v_1(t)$  ( $0 \leq t \leq q^d - 2$ ) 은 다음의 수학식 11과 같이 정의된다.

### 수학식 11

$$v_l(t) = s \left( \left( \frac{q^d - 1}{q - 1} \right) t + l \right) \quad (0 \leq l \leq \frac{q^d - 1}{q - 1} - 1)$$

[0052] 그러면, 수학식 11은 다음의 수학식 12와 같이 표현될 수 있다.

**수학식 12**

[0053] 
$$v_l(t) \equiv \log_{\beta}(N(\alpha^l \beta^t + 1)) \pmod{M}$$

[0054] 여기서  $f_l(x)$ 를 각 음이 아닌 정수  $l$ 에 대해  $\mathbb{F}_q$  상의 차수(degree)가  $d$ 인 다음의 수학식 13의 다항식 (polynomial)이라고 하자.

**수학식 13**

[0055] 
$$\begin{aligned} f_l(x) &= N(\alpha^l x + 1) \\ &= (\alpha^l x + 1)(\alpha^{lq} x + 1) \cdots (\alpha^{lq^{d-1}} x + 1) \\ &= \beta^l x^d + \cdots + \text{Tr}(\alpha^l)x + 1. \end{aligned}$$

[0056] 이제 명백히 다음이 성립한다.

[0057] 
$$v_l(t) \equiv \log_{\beta} f_l(\beta^t) \pmod{M}$$

[0058] 그러면, 각각의  $l$  ( $0 \leq l \leq \frac{q^d-1}{q-1} - 1$ )에 대해 다음의 수학식 14가 유도된다.

**수학식 14**

[0059] 
$$\begin{aligned} f_l(x) &= \beta^l N(x + \alpha^{-l}) \\ &= \beta^l (x + \alpha^{-l})(x + \alpha^{-lq}) \cdots (x + \alpha^{-lq^{d-1}}) \\ &= \beta^l p_l(x)^{\frac{d}{d_l}}. \end{aligned}$$

[0060] 여기서  $p_l(x)$ 은 차수  $d_l$ 인  $-\alpha^{-l}$ 의  $\mathbb{F}_q$  상의 기약 다항식(irreducible polynomial)을 의미하며,  $d_l$ 은  $d$ 의 약수이다.

[0061] 한편,  $l(0 \leq l \leq q^d - 2) \pmod{q^d - 1}$ 를 포함하는  $q$ -원분 잉여류(cyclotomic coset)를  $C_l = \{l, ql, \cdots, q^{d_l-1}l\}$ 라고 하자. 여기서,  $q^j l$ 는  $q^d - 1$ 로 나눈 나머지고,  $d_l$ 은

$$q^{d_l} l \equiv l \pmod{q^d - 1} \text{를 만족하는 최소의 양의 정수이고,} \quad p_l(x) = \prod_{j \in C_l} (x + \alpha^{-j}) \text{이다.}$$

또한,  $l$ 은 법  $q^d - 1$ 에 대한  $C_l$ 의 최소의 양의 정수로 선택할 수 있다.

[0062] 그러면,  $v_l(t) = v_{lq}(t)$ 이고,  $1 \leq l \leq \frac{q^d-1}{q-1} - 1$ 인  $l$ 에 대하여  $p_l(x)$ 은  $\mathbb{F}_q$ 에서

아무런 근(roots)도 갖지 못한다. 나아가,  $l_1 \equiv l_2 \pmod{\frac{q^d-1}{q-1}}$  인 음이 아닌 정수  $l_1, l_2$ 에 대해  $v_{l_1}(t)$  및  $v_{l_2}(t)$  는 순환 비동치(cyclically inequivalent/distinct)이다. 또한,  $v_{\frac{q^d-1}{q-1} - \frac{q^{d-1}-1}{q-1}l}(t) \equiv v_l(t-l+1) \pmod{M}$  이므로,  $v_{\frac{q^d-1}{q-1} - \frac{q^{d-1}-1}{q-1}l}(t)$  와  $v_l(t)$  는 각각의  $l(1 \leq l \leq q)$ 에 대해 순환 동치이다.

[0063] 이제, 이상과 같은 성질을 이용하여 열  $v_l(t)$  ( $0 \leq t \leq q-2$ ) 중 순환 비동치인 열들을 선택하려 한다. 이러한 순환 비동치인 열들을 선택함으로써 수학적 5의 수열로부터 확산 코드 내지 스트림 데이터의 부호화/복호화에 활용될 수 있는 다중 접속 코드들의 집합을 얻을 수 있기 때문이다. 이를 위해서는 정수들의 집합  $l(0 \leq l \leq \frac{q^d-1}{q-1} - 1)$ 에 대한  $q$ -원분 잉여류로부터 각각 하나의 대표원들을 선택한다. 이 경우, 대표원은 각  $q$ -원분 잉여류의 최소 정수인 것이 바람직하다. 여기서,  $q$ -원분 잉여류들은 어떤 동치 관계에 대한 동치류이므로 집합  $l(0 \leq l \leq \frac{q^d-1}{q-1} - 1)$ 을 분할(partition)한다.

[0064] 구체적으로, 집합  $l$ 을 포함하는  $q$ -원분 잉여류는 다음의 수학적 15와 같다.

### 수학적 15

[0065] 
$$\hat{C}_l = \{l, ql, \dots, q^{m_l-1}l\}$$

[0066] 여기서,  $q^j l$  을  $\frac{q^d-1}{q-1}$  로 나눈 나머지고,  $m_l$ 은  $q^{m_l} l \equiv l \pmod{\frac{q^d-1}{q-1}}$  를 만족하는 최소의 양의 정수이다. 또한,  $l$ 은  $\hat{C}_l$  modulo  $\frac{q^d-1}{q-1}$  에서 최소의 양의 정수로 선택될 수 있으며,  $m_l$ 은  $d_l$ 의 약수이다. 따라서, 만약  $q_l(x) = \prod_{j \in \hat{C}_l} (x + \alpha^{-j})$  이면,  $p_l(x) = q_l(x)q_l(x)^{\sigma^{m_l}} q_l(x)^{\sigma^{2m_l}} \dots q_l(x)^{\sigma^{d_l-m_l}}$  이다. 여기서,  $\sigma$ 는  $\mathbb{F}_q$  상의  $\mathbb{F}_{q^d}$ 의 Frobenius 자기동형사상(automorphism)으로서,  $\sigma(a) = a^q$  으로 주어지며, 다음의 수학적 16이 성립한다.

### 수학적 16

[0067] 
$$q_l(x)^{\sigma^{im_l}} = \prod_{j \in \hat{C}_l} (x + \alpha^{-jq^{im_l}}) \quad (0 \leq i \leq \frac{d_l}{m_l} - 1)$$

[0068] 이제,  $l(1 \leq l \leq \frac{q^d-1}{q-1})$ 으로 구성된 집합에 대해 범  $\frac{q^d-1}{q-1}$ 에 대한  $q$ -원분 잉여류의 대표값의 집합에 대응하는 수열의 열  $v_l(t)$ 의 상수 곱(constant multiples)으로 구성된 주기  $q-1$ 의  $M$ -진 수열의 족(family)  $\Sigma$

을 구성하고자 한다.

[0069] 각각의  $q$ -원분 잉여류의 최소 정수들을 모아 놓은 집합을  $\Lambda$  로 정의하자.  $|\Lambda|$  는  $q$ -원분 잉여류의 개수이며, 이는 또한  $x^{\frac{q^d-1}{q-1}} - 1$  의 최고차항의 계수가 1인 기약 인자(mononic irreducible factor)들의 개수와도 같다. 또한,  $p(x) = x^e + \dots + (-1)^e b$  를  $x^{\frac{q^d-1}{q-1}} - 1$  의 최고차항의 계수가 1인 기약 인자라고 하면,  $e|d$  이고  $b^{\frac{d}{e}} = 1$  가 성립한다.

[0070] 이하에서는  $d$ 가 다음의 수학적 17의 조건을 만족한다고 가정하자.

### 수학적 17

[0071] 
$$(d, q-1) = 1, \quad d < \frac{\sqrt{q} - \frac{2}{\sqrt{q}} + 1}{2}$$

[0072] 수학적 17에서  $d$ 와  $q-1$ 은 서로 소임을 의미하며, 수열 족에 제약(restriction)을 가하기 위해 가정되었다.

[0073]  $l_1, l_2$ 를 집합  $\Lambda \setminus \{0\}$ 의 원소라고 하고,  $\tau(0 \leq \tau \leq q-2)$ 를 정수라고 하자. 만약  $l_1 = l_2$  이 아니거나  $\tau = 0$  이 아니면,  $p_{l_1}(x)$ 과  $\beta^{-\tau d_{l_2}} p_{l_2}(\beta^\tau x)$ 는  $\mathbb{F}_q$  상의 서로 다른 기약 다항식(distinct irreducible polynomials)이다. 여기서,  $\beta^{-\tau d_{l_2}} p_{l_2}(\beta^\tau x)$ 은 다음의 수학적 18과 같이 정리된다.

### 수학적 18

[0074] 
$$\begin{aligned} & \beta^{-\tau d_{l_2}} p_{l_2}(\beta^\tau x) \\ &= (x + \alpha^{-l_2} \beta^{-\tau})(x + \alpha^{-l_2 q} \beta^{-\tau}) \dots (x + \alpha^{-l_2 q^{d_{l_2}-1}} \beta^{-\tau}) \end{aligned}$$

[0075] 그러면, 이상에서 구성한 주기  $q-1$ 의  $M$ -진 수열로 구성된 수열 족  $\Sigma$ 는 다음의 수학적 19와 같이 정의된다.

### 수학적 19

[0076] 
$$\Sigma = \{cv_l(t) | 1 \leq c \leq M-1, l \in \Lambda \setminus \{0\}\}$$

[0077] 이상에서 설명한 수열 족의 생성 방법을 도 1과 도 2를 참조하여 정리하면 다음과 같다. 도 1은 본 발명의 실시예에 따른 통신 시스템의 채널 확산을 위한 수열 족을 생성하는 방법을 도시한 흐름도로서, 다음과 같은 단계들을 포함한다.

[0078] 110 단계에서 유한체 상의 로그함수를 이용하여  $q^d-1$ ( $q$ 는 소수승,  $d$ 는 2 이상인 정수)의 주기를 갖는  $M$ -진( $M$ 은  $q-1$ 의 약수) 수열을 생성한다. 여기서,  $M$ -진 수열은  $M$ -진 시뮬니코프 수열을 활용할 수 있다. 이러한 110 단계는 도 2의 수열 생성부(210)에서 수행되는 것으로, 수열 생성부(210)는 전자적 형태의 정보 및 수학적식을 처리할 수 있는 처리기(processor) 및 이러한 연산에 필요한 기억공간(memory)을 통해 구현될 수 있으며, 필요에 따라서는 처리기와 기억공간 간의 데이터 처리를 적절하게 제어할 수 있는 제어기(controller)가 활용될

수도 있을 것이다. 이러한 처리기, 기억공간 및 제어기는 본 발명이 속하는 기술분야의 활용 환경이나 동작 환경을 고려하여 통상의 기술자에 의해 적절하게 선택될 수 있을 것이다. 나아가, 이러한 수열 생성부(210)를 구현함에 있어서 이상에서 예시된 하드웨어들을 제어하기 위한 부가적인 소프트웨어 코드(code)도 활용될 수 있을 것이다.

[0079] 120 단계에서는 110 단계에서 생성한 M-진 수열을 주기  $q-1$ 을 기준으로 구분하여 행렬로 배열한다. 앞서 검토

하였듯이 이러한 행렬은 M-진 수열을  $(q-1) \times \left(\frac{q^d-1}{q-1}\right)$  (d는 1보다 큰 양의 정수)의 형태로 배열한 것이 바람직하다.

[0080] 130 단계에서는 배열된 행렬로부터 순환 비동치인 대표열들을 선택하여 저장한다. 앞서 검토하였듯이 이러한 순환 비동치인 대표열은 q-원분 잉여류의 최소 정수인 것이 바람직하다.

[0081] 이상의 120 단계 및 130 단계에서 M-진 수열을 주기를 기준으로 구분하여 행렬로 배열하고, 배열된 행렬로부터 순환 비동치인 대표열들을 선택하는 과정은 도 2의 연산부(220)에서 수행된다. 이러한 연산부(220) 역시 전자적 형태의 정보 및 수학식을 처리할 수 있는 처리기와 이들 하드웨어를 제어할 수 있는 제어기를 활용하여 구현될 수 있다. 한편, 배열된 행렬과 선택된 대표열들을 저장하기 위해서는 도 2의 저장부(230)가 필요하다. 즉, 행렬의 배열과 대표열의 선택 과정에서 연산에 필요한 기억공간으로서 레지스터(register) 등과 같은 하드웨어로 구현될 수 있는 저장부(230)가 활용된다. 또한, 이상에서 예시된 하드웨어들을 제어하기 위한 부가적인 소프트웨어 코드가 활용될 수 있음은 당연하다.

[0082] 마지막으로, 140 단계에서는 130 단계에서 저장된 대표열들을 상수배하여 수열 족을 생성한다. 이러한 140 단계는 도 2의 수열 족 생성부(240)에 의해 수행되는데, 수열 족 생성부(240)는 대표열들의 상수배를 위해 연산을 처리할 수 있는 처리기와 이를 저장하기 위한 기억공간과 같은 하드웨어로 구현될 수 있다.

[0083] 이 때, 생성된 수열 족의 최대상관수(maximum correlation magnitude)는  $(2d-1)\sqrt{q}+1$  (d는 1보다 큰 양의 정수)를 상계(upper bound)로 갖는 것이 바람직하다. 나아가, 생성된 수열 족의 점근적 크기는 q의 정수  $\frac{(M-1)q^{d-1}}{d}$  (d는 1보다 구체적으로는 d-1 승을 의미한다.)에 비례하게 되며, 보다 구체적으로는  $\frac{(M-1)q^{d-1}}{d}$  (d는 1보다 큰 양의 정수)인 것이 바람직하다. 이러한 수열 족의 최대상관수 및 점근적 크기에 관하여는 이하에서 보다 구체적으로 설명한다.

[0084] 주기가  $q-1$ 인 M-진 수열의 수열 족  $\Sigma = \{cv_l(t) | 1 \leq c \leq M-1, l \in \Lambda \setminus \{0\}\}$ 에 대해 다음의 수학적 식 20이 성립한다.

### 수학식 20

[0085]  $\delta_{\max}(\Sigma) \leq (2d-1)\sqrt{q}+1$

[0086] 이러한 수학적 식 20은 다음과 같이 유도될 수 있다.

[0087] 우선  $l_1 \neq l_2 (l_1, l_2 \in \Lambda \setminus \{0\})$  또는  $\tau$ 가  $1 \leq \tau \leq q-2$ 의 범위 내에 있다고 가정하자. 그러면,  $p_{l_1}(x)$ 와  $\beta^{-\tau d_{l_2}} p_{l_2}(\beta^\tau x)$ 는 앞서 설명한 수학적 식 18에 의해  $\mathbb{F}_q$  상의 서로 다른 기약 다항식(distinct irreducible polynomials)임을 알 수 있다. 이어서, 수열 족  $\Sigma$ 에서 수열  $c_1 v_{l_1}(t)$ 와  $c_2 v_{l_2}(t)$  간의 상호상관 함수(cross-correlation function)  $R(\tau) = R_{c_1, l_1, c_2, l_2}(\tau)$ 는 다음의 수학적 식 21과 같이 주어진다.

### 수학식 21

$$\begin{aligned}
 R(\tau) &= \sum_{t=0}^{q-2} w_M^{c_1 v_{l_1}(t) - c_2 v_{l_2}(t+\tau)} \\
 &= \sum_{t=0}^{q-2} \psi^{c_1}(f_{l_1}(\beta^t)) \psi^{M-c_2}(f_{l_2}(\beta^{t+\tau})) \\
 &= \sum_{x \in \mathbb{F}_q} \psi_1(p_{l_1}(x)) \psi_2(\beta^{-\tau d_{l_2}} \times \beta^{\tau d_{l_2}} p_{l_2}(\beta^{\tau} x)) - 1
 \end{aligned}$$

[0088]

[0089] 여기서,  $\psi_1 = \psi^{c_1 \frac{d}{d_{l_1}}}$  이고,  $\psi_2 = \psi^{c_2 \frac{d}{d_{l_2}}}$  이다.  $(d, q-1) = 1$  이기 때문에  $c_1 \frac{d}{d_{l_1}}$  및  $c_2 \frac{d}{d_{l_2}}$  는 모두  $M$ 에 의해 약분이 불가능하다. 따라서,  $\psi_1$ 과  $\psi_2$ 는 모두 자명한 곱지표가 아니다.

[0090] 한편,  $f_1(x), \dots, f_m(x)$ 의 차수가  $d_1, \dots, d_m$  이고,  $f_j(x) (j = 1, \dots, m)$ 의  $\mathbb{F}_q$ 에서의 서로 다른 근의 개수가  $e_j$ 인, 최고차항의 계수가 1인  $\mathbb{F}_q$ 상의 기약 다항식(mononic irreducible polynomials)이라고 하자. 또한,  $\psi_1, \dots, \psi_m$ 를  $\psi_j(0) = 1 (j = 1, \dots, m)$ 인  $\mathbb{F}_q$ 의 자명하지 않은 곱 지표(nontrivial multiplicative characters)라고 하자. 그러면,  $a_1, \dots, a_m \in \mathbb{F}_q^\times$ 에 대해 다음의 수학식 22를 추정할 수 있다.

### 수학식 22

$$\begin{aligned}
 &\left| \sum_{x \in \mathbb{F}_q} \psi_1(a_1 f_1(x)) \cdots \psi_m(a_m f_m(x)) \right| \\
 &\leq \left( \sum_{j=1}^m d_j - 1 \right) \sqrt{q} + \sum_{j=1}^m e_j.
 \end{aligned}$$

[0091]

[0092] 이제 수학식 21 및 수학식 22에 의해 절대값은 다음의 수학식 23과 같이 정리될 수 있다.

### 수학식 23

$$\begin{aligned}
 &\left| \sum_{x \in \mathbb{F}_q} \psi_1(p_{l_1}(x)) \psi_2(\beta^{-\tau d_{l_2}} \times \beta^{\tau d_{l_2}} p_{l_2}(\beta^{\tau} x)) \right| \\
 &\leq (d_{l_1} + d_{l_2} - 1) \sqrt{q} \\
 &\leq (2d - 1) \sqrt{q}.
 \end{aligned}$$

[0093]

[0094] 그러면,  $c_1 \neq c_2$  이고  $l_1 = l_2$  이며  $\tau = 0$  인 경우에 있어 상호-상관 함수는 다음의 수학식 24와 같이 정리된다.

수학식 24

$$\begin{aligned} R(\tau) &= \sum_{t=0}^{q-2} w_M^{(c_1-c_2)v_{l_1}(t)} \\ &= \sum_{x \in \mathbb{F}_q} \psi^*(p_{l_1}(x)) - 1 \end{aligned}$$

[0095]

여기서,  $(c_1 - c_2) \frac{d}{d_{l_1}}$  는  $\mathbb{M}$ 에 의해 약분될 수 없으며,  $\psi^* = \psi^{(c_1-c_2) \frac{d}{d_{l_1}}}$  는 자명한 곱지표가 아니다. 따라서, 통상적인 Weil's 정리에 의해 다음의 수학식 25가 성립한다.

[0096]

수학식 25

$$\begin{aligned} |R(\tau)| &\leq (d_{l_1} - 1)\sqrt{q} + 1 \\ &\leq (d - 1)\sqrt{q} + 1. \end{aligned}$$

[0097]

이제, 수열 족  $\Sigma$ 에 속한 수열들이 순환 비동치임을 보다 구체적으로 살펴보자.

[0098]

만약  $c_1 v_{l_1}(t)$  와  $c_2 v_{l_2}(t)$  가 순환 동치이면,  $\tau(0 \leq \tau \leq q-2)$ 에 대해  $c_1 v_{l_1}(t) = c_2 v_{l_2}(t + \tau)$  이고, 그 결과 다음의 수학식 26이 성립한다.

[0099]

수학식 26

$$\begin{aligned} q - 1 &= \sum_{t=0}^{q-2} w_M^{c_1 v_{l_1}(t) - c_2 v_{l_2}(t + \tau)} \\ &= \left| \sum_{t=0}^{q-2} w_M^{c_1 v_{l_1}(t) - c_2 v_{l_2}(t + \tau)} \right| \\ &\leq \left| \sum_{x \in \mathbb{F}_q} \psi_1(p_{l_1}(x)) \psi_2(\beta^{-\tau d_{l_2}} \times \beta^{\tau d_{l_2}} p_{l_2}(\beta^{\tau} x)) \right| + 1 \\ &\leq (2d - 1)\sqrt{q} + 1. \end{aligned}$$

[0100]

if  $(c_1, l_1) \neq (c_2, l_2)$

[0101]

여기서,  $\psi_1 = \psi^{c_1 \frac{d}{d_{l_1}}}$  이고,  $\psi_2 = \psi^{c_2 \frac{d}{d_{l_2}}}$  이다. 앞서 수학식 17의 가정에 따르면 이상의 과정은 불가능하다. 따라서,  $c_1 v_{l_1}(t)$  와  $c_2 v_{l_2}(t)$  는 같다.

[0102]

이제 수열 족  $\Sigma$ 의 크기에 대한 구체적이지는 않지만 정확한 표현을 산출하도록 하겠다. 수열 족

[0103]

$\Sigma = \{cv_l(t) | 1 \leq c \leq M-1, l \in \Lambda \setminus \{0\}\}$  의 크기는 다음의 수학식 27과 같이 표현될 수 있다.

**수학식 27**

$$|\Sigma| = (M-1)(|\Lambda|-1)$$

여기서,  $x^{\frac{q^d-1}{q-1}} - 1$  의 최고차항의 계수가 1인 기약 인자의 개수  $|\Lambda|$  는 다음의 수학식 28과 같이 주어진다.

**수학식 28**

$$\sum_{e|d} \frac{1}{e} \sum_{\substack{r \in A_e \\ m_{re}=1}} \phi(r)$$

이제,  $q \rightarrow \infty$  일 때 수열 족  $\Sigma$  의 점근적 크기가 어떠한 값이 되는지에 대하여 검토하도록 하겠다. 어떠한 원소(element)  $b \in \mathbb{F}_q^\times$  에 대해 상수항(constant term)이  $(-1)^f b$  이고 차수가 f인  $\mathbb{F}_q$  상의 최고차항의 계수가 1인 기약 다항식의 개수를  $N(f, b, q)$  라고 하자. 그러면, 다음의 수학식 29가 성립한다.

**수학식 29**

$$\left| N(f, b, q) - \frac{q^f}{f(q-1)} \right| \leq \frac{2}{f} q^{\frac{f}{2}}$$

이상의 수학식 29로부터 다음의 수학식 30이 유도된다.

**수학식 30**

$$||\Lambda| - \sum_{e|d} \frac{q^e}{e(q-1)}| \leq 2 \sum_{e|d} \frac{q^{e/2}}{e}$$

이는  $|\Lambda| - 1 \sim \frac{q^{d-1}}{d}$ , as  $q \rightarrow \infty$  를 의미하므로, 수열 족  $\Sigma$  에서  $q \rightarrow \infty$  일 때의 점근적(asymptotic) 크기는 다음의 수학식 31과 같다.

**수학식 31**

$$|\Sigma| \sim \frac{(M-1)q^{d-1}}{d}, \text{ as } q \rightarrow \infty$$

[0113] 이제  $d$ 를 가령  $p$ 의 임의의 거듭제곱  $P^a$  ( $a \geq 1$ ) 으로 선택하면,  $q=p^n$  ( $n \geq 2(a+1)$ ) 인 모든  $q$ 에 대하여 수학적 17의 조건을 만족하므로,  $q \rightarrow \infty$  일 때 수열 족  $\Sigma$ 의 점근적 크기가 다음의 수학적 32임을 알 수 있다.

### 수학적 32

$$\frac{(M-1)q^{d-1}}{d} = \frac{(M-1)(L+1)^{p^a-1}}{p^a}$$

[0114]

[0115] 여기서,  $L=q-1$ 은 수열 족  $\Sigma$ 의 주기를 나타낸다.

[0116] 상기된 본 발명의 실시예가 제안하고 있는 수열 족의 크기를 검토하면 주기  $L$ 에 대한 임의의 거듭제곱의 크기가 됨을 확인할 수 있다. 이러한 수열 족의 크기는 이제까지 알려진 가장 좋은 결과인  $L^3$  정도를 크게 증가하는 수치이다. 도 5는 종래에 알려진 방법에 의해 생성된 수열 족들의 특성을 비교하여 설명하기 위한 도면으로서, 수열 족의 크기(family size)를 쉽게 비교해 볼 수 있다.

[0117] 따라서, 상기된 본 발명의 실시예들에 따르면 채널 확산 기술을 사용하는 통신 시스템의 폭발적인 수요 증가에 부응하여 하나의 채널에 포함될 수 있는 송신 데이터의 수를 비약적으로 증가시킴으로써 채널 내 데이터 포화의 한계를 극복하고, 낮은 상관 성질로 인해 불법적인 무선 통신 감청이나 해킹에 강인한 특성을 갖는 수열 족을 제공하는 것이 가능하다.

[0118] 이하에서는 이상과 같이 제안된 수열 족을 사용하여 대역 확산 통신 시스템에서 활용하는 방법에 대해 설명한다.

[0119] 도 3은 본 발명의 다른 실시예에 따른 통신 시스템의 채널 확산을 위한 일련의 통신 과정을 설명하기 위한 도면으로서 송신측으로부터 신호를 부호화하여 전송한 후, 수신측에서 수신된 신호를 다시 복호화하는 과정을 도시하고 있다.

[0120] 우선, RF 발진기(310)는 무선 통신을 위한 주파수를 생성하여 입력 신호를 적재한다. 본 실시예는 대역 확산 통신 시스템을 가정하고 있으므로 PN 코드 발생기(321)를 통해 생성된 유사잡음코드(pseudo random noise code; PN 코드)를 송신하여 원신호를 확산시킨다. 이어서, 전력 증폭기(330)를 통해 증폭된 신호는 안테나(341)를 통해 송신된다.

[0121] 이제 수신측에서는 안테나(342)를 통해 확산 신호를 수신한 후 복호화하게 된다. 이 때, PN 코드 발생기(322)는 송신측의 PN 코드 발생기(321)와 동일한 유사잡음코드를 생성하게 되는데 이렇게 생성된 코드를 송신함으로써 원신호를 복원할 수 있음은 앞서 수학적 1을 통해 설명한 바 있다.

[0122] 이상의 대역 확산 통신 시스템에서는 본 발명의 실시예에 따른 수열 족을 활용함으로써 보다 많은 동시 접속자를 수용할 수 있게 된다. 즉, 본 발명의 실시예에 따르면 수열 족의 크기가 매우 큰 값을 가질 수 있기 때문에 다수의 사용자 신호를 수용하기에 적합하다.

[0123] 도 4a 및 도 4b는 각각 본 발명의 다른 실시예에 따른 통신 시스템의 채널 확산을 위한 확산 신호의 생성 장치 및 확산 신호를 역확산하는 장치를 도시한 도면으로서, 도 3의 구성을 보다 구체적으로 설명하기 위한 것이다.

[0124] 우선 도 4a는 송신측에서 통신 시스템의 채널 확산을 위한 확산 신호를 생성하는 장치를 도시한 것으로, 다음과 같은 구성을 포함한다.

[0125] 입력부(410, 420)는 음성 신호를 입력받아 디지털 변조한다. 이 때의 원신호(41a)는 협대역 신호에 해당한다.

[0126] 확산 코드 생성부(435)는 이상의 실시예들을 통해 제시하고 있는 수열 족(437)으로부터 확산 코드를 생성한다. 구체적으로 상기 수열 족은 유한체 상의 로그함수를 이용하여  $q^d-1$ ( $q$ 는 소수승,  $d$ 는 2 이상인 정수)의 주기를 갖는  $M$ -진( $M$ 은  $q-1$ 의 약수) 수열을 생성하고,  $M$ -진 수열을  $q-1$  주기를 기준으로 구분하여 행렬로 배열하고, 배열된 행렬으로부터 순환 비동치인 대표열들을 선택하여 저장하고, 저장된 대표열들을 상수 배함으로써 생성될 수 있다. 또한, 상기 수열 족의 점근적 크기는  $q$ 의 정수승(보다 구체적으로는  $q$ 의  $d-1$  승

을 의미한다.)에 비례하는 것이 바람직하다. 나아가 이상의 M-진 수열은 M-진 시퀀스 코프 수열이고, 순환 비

동치인 대표열은  $q$ -원분 잉여류의 최소 정수이며, 상기 행렬은 M-진 수열을  $(q-1) \times (\frac{q^d-1}{q-1})$  (d는 1보다 큰 양의 정수)의 형태로 배열한 것이 바람직하다.

[0127] 확산 신호 생성부(430)는 입력부(410, 420)를 통해 입력된 신호에 확산 코드 생성부(435)를 통해 생성된 확산 코드를 승산하여 대역폭을 확산시킴으로써 확산 신호를 생성한다. 따라서, 안테나(441)을 통해 송신되는 확산 신호는 도 4a에 도시된 바와 같이 협대역 신호인 원신호(41a)와는 달리 광대역 신호(41b)로 확산되었음을 알 수 있다.

[0128] 다음으로 도 4b는 수신측에서 통신 시스템의 채널 확산을 위한 확산 신호를 역확산(despreading)하는 장치를 도시한 것으로, 다음과 같은 구성을 포함한다.

[0129] 수신부(442)는 확산(spreading) 신호를 수신한다. 이 때, 수신되는 신호는 확산 신호(41b) 외에 잡음 신호(42a)를 포함한다.

[0130] 이제 수신된 신호들(확산 신호 및 잡음 신호)을 복원하기 위해 확산 코드 생성부(455)는 수열 족(457)으로부터 확산 코드를 생성한다. 이 때의 확산 코드가 송신측의 확산 코드와 동일한 코드이며 동일한 과정에 의해 생성되었음은 당연하다.

[0131] 신호 복원부(450)는 수신된 확산 신호에 확산 코드 생성부(455)를 통해 생성된 확산 코드를 승산하여 대역폭을 역확산시킴으로써 확산 신호의 원본 신호(41a)를 복원한다. 물론 역확산 과정에서 잡음 신호 또한 확산 코드와 승산되게 되는데, 앞서 수학식 1을 통해 설명한 바와 같이 이러한 확산 코드에 의해 잡음 신호는 원신호와 더욱 차별화되게 된다. 따라서, 잡음 신호의 영향력은 매우 희석(작아지게 된다.)되게 된다. 도 4b에서는 역확산 이후 2개의 신호(확산 신호 및 잡음 신호)가 어떻게 변조되었는지를 도시하고 있다. 즉, 광대역의 확산 신호(41b)는 역확산에 의해 다시 협대역의 원신호(41a)로 복원되었고, 잡음 신호(42a)는 여전히 광대역 신호(42b)로 존재함을 알 수 있다.

[0132] 상기된 본 발명의 다른 실시예들에 따르면 채널 확산 기술을 사용하는 통신 시스템의 폭발적인 수요 증가에 부응하여 하나의 채널에 포함될 수 있는 송신 데이터의 수를 비약적으로 증가시킴으로써 채널 내 데이터 포화의 한계를 극복하고, 낮은 상관 성질로 인해 불법적인 무선 통신 감청이나 해킹에 강인한 특성을 갖는 대역 확산 통신 시스템을 구축하는 것이 가능하다.

[0133] 한편, 본 발명은 컴퓨터로 읽을 수 있는 기록 매체에 컴퓨터가 읽을 수 있는 코드로 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록 매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다.

[0134] 컴퓨터가 읽을 수 있는 기록 매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광 데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들어 인터넷을 통한 전송)의 형태로 구현하는 것을 포함한다. 또한, 컴퓨터가 읽을 수 있는 기록 매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산 방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다. 그리고 본 발명을 구현하기 위한 기능적인(functional) 프로그램, 코드 및 코드 세그먼트들은 본 발명이 속하는 기술 분야의 프로그래머들에 의하여 용이하게 추론될 수 있다.

[0135] 이상에서 본 발명에 대하여 그 다양한 실시예들을 중심으로 살펴보았다. 본 발명에 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

## 부호의 설명

[0136] 210 : 수열 생성부

220 : 연산부

240 : 수열 족 생성부

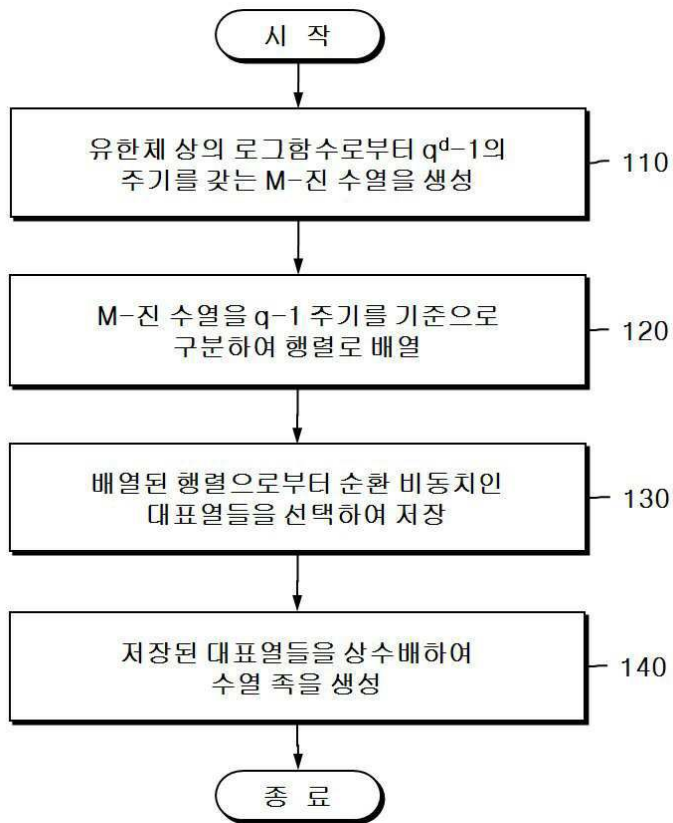
230 : 저장부

310 : RF 발진기

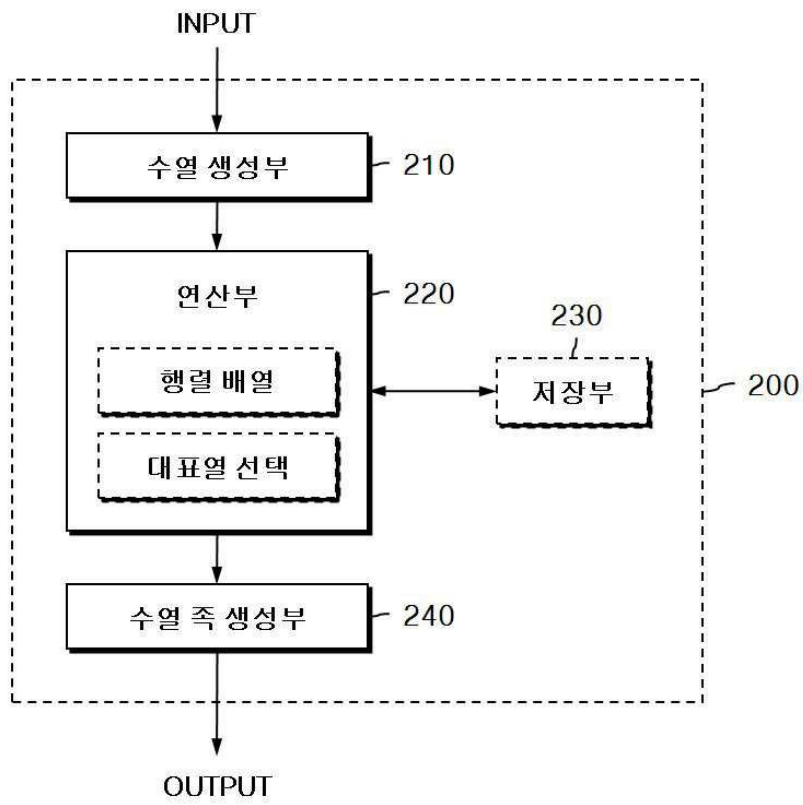
321, 322 : PN 코드 발생기  
 330 : 전력 증폭기  
 341, 342 : 안테나  
 410 : 입력부  
 420 : 디지털 변조기  
 435, 455 : 확산 코드 생성부  
 437, 457 : 수열 족  
 430 : 대역 확산부  
 450 : 역확산부(신호 복원부)  
 441, 442 : 안테나  
 460 : 디지털 복조부  
 470 : 출력부

## 도면

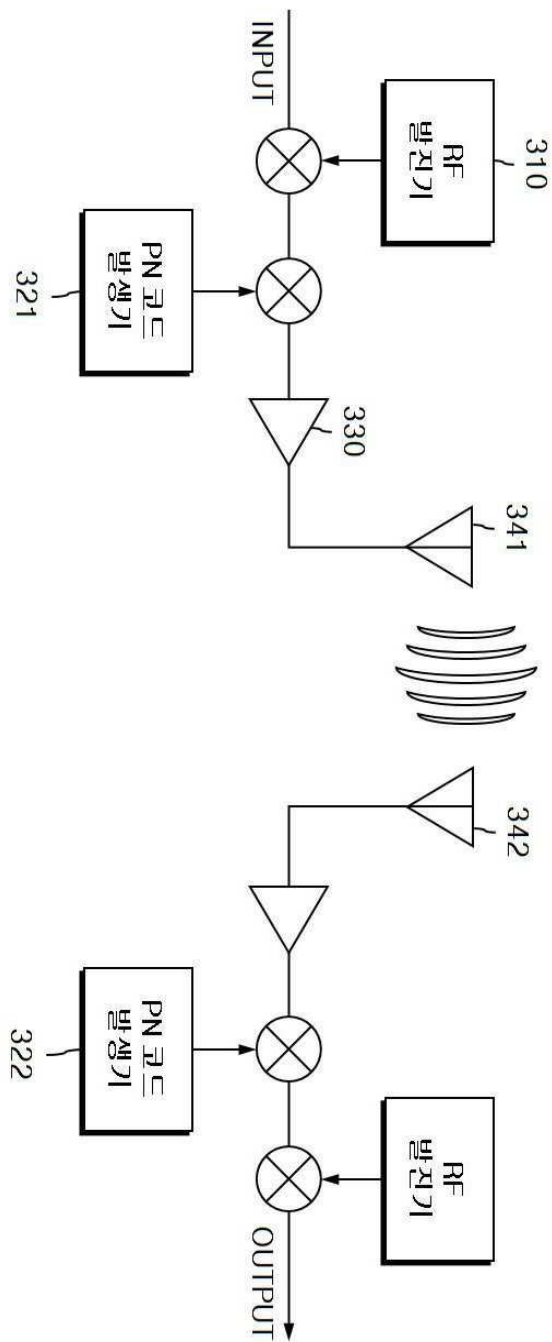
### 도면1



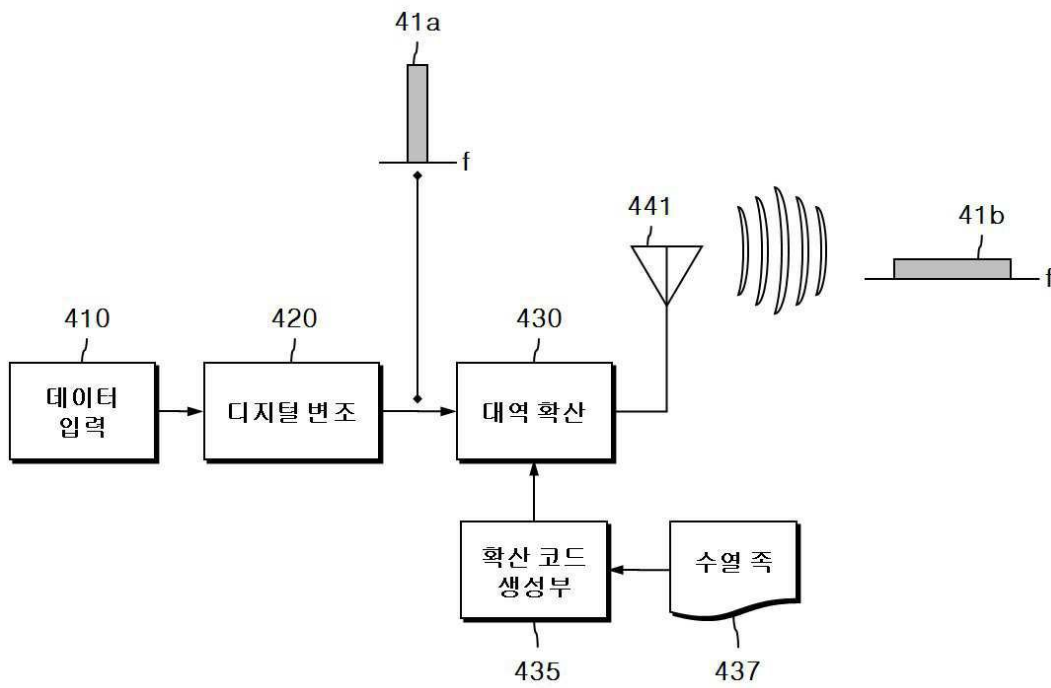
도면2



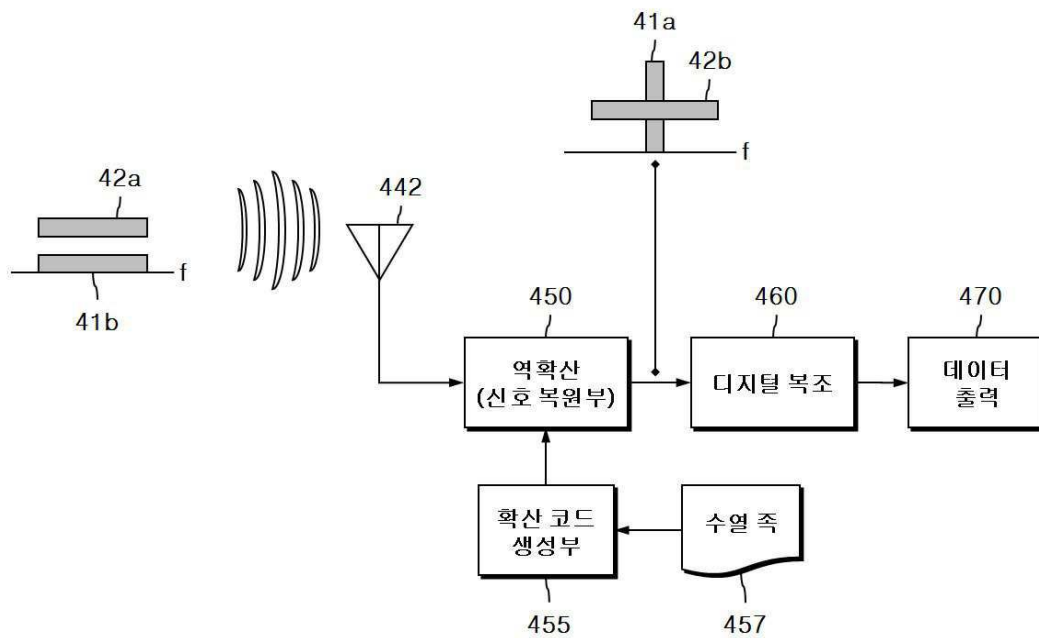
도면3



도면4a



도면4b



도면5

|                              | Period $L$                                                   | Alphabet             | $C_{\max}$          | Family size                                                          |
|------------------------------|--------------------------------------------------------------|----------------------|---------------------|----------------------------------------------------------------------|
| Trachtenberg                 | $p^m - 1, m \text{ odd}$                                     | $p$                  | $\sqrt{p(L+1)} + 1$ | $L + 2$                                                              |
| Helleseth                    | $p^m - 1, m \text{ even}$<br>$p^{m/2} \not\equiv 2 \pmod{3}$ | $p$                  | $2\sqrt{L+1} + 1$   | $L + 2$                                                              |
| Sidelnikov                   | $p^m - 1$                                                    | $p$                  | $\sqrt{L+1} + 1$    | $L + 1$                                                              |
| Bent                         | $p^m - 1, m \text{ even}$                                    | $p$                  | $\sqrt{L+1} + 1$    | $\sqrt{L+1}$                                                         |
| Kumar, Moreno                | $p^m - 1$                                                    | $p$                  | $\sqrt{L+1} + 1$    | $L + 1$                                                              |
| Gong                         | $(p^m - 1)^2$                                                | $p$                  | $2\sqrt{L} + 3$     | $\sqrt{L}$                                                           |
| $\mathbb{Z}_4$ Family $S(0)$ | $2^m - 1$                                                    | 4                    | $\sqrt{L+1} + 1$    | $L + 2$                                                              |
| $\mathbb{Z}_4$ Family $S(1)$ | $2^m - 1$                                                    | 4                    | $2\sqrt{L+1} + 1$   | $\geq L^2 + 3L + 2$                                                  |
| $\mathbb{Z}_4$ Family $S(2)$ | $2^m - 1$                                                    | 4                    | $4\sqrt{L+1} + 1$   | $\geq L^3 + 4L^2 + 5L + 2$                                           |
| $\tilde{\mathcal{F}}_r$      | $p$                                                          | $M$                  | $2\sqrt{L} + 5$     | $\left(\frac{L+1}{2}\right) \cdot (M-1)$                             |
| $\mathcal{F}_r$              | $p$                                                          | $M$                  | $3\sqrt{L} + 4$     | $M-1 + \frac{(M-1)^2(L-1)}{2}$                                       |
| $\tilde{\mathcal{F}}_s$      | $p^m - 1$                                                    | $M$                  | $2\sqrt{L+1} + 6$   | $(M-1) \cdot \frac{L}{2} + \left\lfloor \frac{M-1}{2} \right\rfloor$ |
| $\mathcal{L}$                | $p^m - 1$                                                    | $M$                  | $3\sqrt{L+1} + 5$   | $\frac{(M-1)^2(L-2)}{2} + \frac{M(M-1)}{2}$                          |
| $\mathcal{V}^{(c_1)}$        | $p^m - 1$                                                    | $M > 2 \text{ even}$ | $2\sqrt{L+1} + 2$   | $L + M - 1$                                                          |
| $\mathcal{V}$                | $p^m - 1$                                                    | $M$                  | $3\sqrt{L+1} + 1$   | $\left(\frac{L}{2} + 1\right) \cdot (M-1)$                           |
| $\tilde{\mathcal{U}}$        | $p^m - 1$                                                    | $M \text{ even}$     | $2\sqrt{L+1} + 6$   | $(L+1) \cdot \frac{M}{2} - 1$                                        |
| $\mathcal{U}$                | $p^m - 1$                                                    | $M$                  | $3\sqrt{L+1} + 5$   | $\frac{M(M-1)(L-1)}{2} + M - 1$                                      |