



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2016년04월27일
(11) 등록번호 10-1615744
(24) 등록일자 2016년04월20일

- (51) 국제특허분류(Int. Cl.)
H04L 27/34 (2006.01) H04B 10/70 (2013.01)
H04L 9/08 (2006.01)
(52) CPC특허분류
H04L 27/34 (2013.01)
H04B 10/70 (2013.01)
(21) 출원번호 10-2015-0020717
(22) 출원일자 2015년02월11일
심사청구일자 2015년02월11일
(65) 공개번호 10-2015-0097401
(43) 공개일자 2015년08월26일
(30) 우선권주장
1020140018392 2014년02월18일 대한민국(KR)
(56) 선행기술조사문헌

Kentaro Kato et al., "Quantum Detection and Mutual Information for QAM and PSK Signals", IEEE TRANSACTIONS ON COMMUNICATIONS, VOL. 47, NO. 2, 1999.02*

Atsushi Waseda et al., "Quantum detection of wavelength division multiplexing optical coherent signals in lossy channels", 2010 International Conference on Availability, Reliability and Security, 2010*

*는 심사관에 의하여 인용된 문헌

- (73) 특허권자
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
고영채
서울특별시 송파구 잠실로 62, 327동 702호 (잠실동, 트리지움아파트)
김영준
서울특별시 양천구 신정로 293, 108동 503호 (신정동, 신트리1단지아파트)
(74) 대리인
특허법인엠에이피에스

전체 청구항 수 : 총 6 항

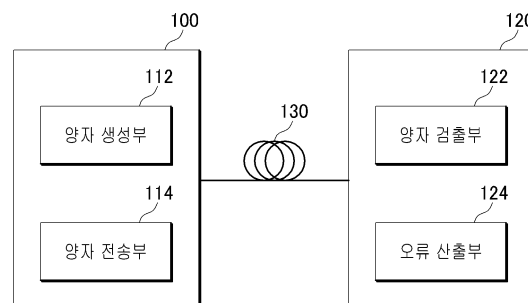
심사관 : 남인호

(54) 발명의 명칭 양자 통신을 위한 시스템 및 양자 신호 송수신 방법

(57) 요약

본 발명은 양자 통신을 위한 양자 송신 장치의 양자 신호 송신 방법에 있어서, M배열 원형 직교 진폭 변조(Circular QAM) 결맞음 상태 세트를 구성하는 단계, 송신하고자 하는 메시지에 따라 결맞음 상태 세트 내 M개의 결맞음 상태 중 어느 하나를 선택하는 단계, 결맞음 상태 세트를 공유하는 양자 수신장치로 선택된 결맞음 상태를 송신하는 단계를 포함하고 구성하는 단계는 가변적으로 선택되는 에너지 내에서 결맞음 상태간 최소 유클리드 거리가 최대화 되도록 구성하는 양자 신호 송신 방법을 제공한다.

대 표 도 - 도1



(52) CPC특허분류

H04L 9/0852 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 12-911-04-003

부처명 미래창조과학부

연구관리전문기관 한국방송통신전파진흥원

연구사업명 방송통신인프라원천기술개발사업

연구과제명 양자 통신 및 양자 정보 처리를 위한 기술 개발

기 여 율 1/1

주관기관 고려대학교 산학협력단

연구기간 2013.03.01 ~ 2014.02.28

공지예외적용 : 있음

명세서

청구범위

청구항 1

양자 통신을 위한 양자 송신 장치의 양자 신호 송신 방법에 있어서,

M배열 원형 직교 진폭 변조(Circular QAM) 결맞음 상태 세트를 구성하는 단계;

송신하고자 하는 메시지에 따라 상기 결맞음 상태 세트 내 M개의 결맞음 상태 중 어느 하나를 선택하는 단계; 및

상기 결맞음 상태 세트를 공유하는 양자 수신장치로 상기 선택된 결맞음 상태를 송신하는 단계를 포함하고,

상기 구성하는 단계는 가변적으로 선택되는 에너지 내에서 상기 결맞음 상태간 최소 유클리드 거리가 최대화 되도록 구성하는 양자 신호 송신 방법.

청구항 2

제 1항에 있어서,

상기 M이 8이고, 상기 결맞음 상태간 최소 유클리드 거리가 2α 인 경우,

상기 구성하는 단계는

제 1원의 반지름을 $\sqrt{2}\alpha$ 로 설정하는 단계; 및

상기 제 1원과 중심점을 공유하는 제 2원의 반지름을 $(1 + \sqrt{3})\alpha$ 로 설정하는 단계를 포함하고,

상기 결맞음 상태 세트 내 8개의 결맞음 상태는

$$|\psi_1\rangle = |\alpha(1+j)\rangle$$

$$|\psi_2\rangle = |\alpha(-1+j)\rangle$$

$$|\psi_3\rangle = |\alpha(-1-j)\rangle$$

$$|\psi_4\rangle = |\alpha(1-j)\rangle$$

$$|\psi_5\rangle = |\alpha(1+\sqrt{3})\rangle$$

$$|\psi_6\rangle = |\alpha j(1+\sqrt{3})\rangle$$

$$|\psi_7\rangle = |-\alpha(1+\sqrt{3})\rangle$$

$$|\psi_8\rangle = |-\alpha j(1+\sqrt{3})\rangle \text{ 인 양자 신호 송신 방법. (단, } \alpha \text{ 는 가변적으로 선택되는 에너지의 크기임)}$$

청구항 3

제 1항에 있어서,

상기 M이 16이고, 상기 결맞음 상태간 최소 유클리드 거리가 2α 인 경우,

상기 구성하는 단계는 제 1원의 반지름을 $\sqrt{2}\alpha$ 로 설정하는 단계;

제 2원의 반지름을 $(1 + \sqrt{3})\alpha$ 로 설정하는 단계;

제 3원의 반지름을 $\sqrt{r_2^2 + 2^2 - 4r_2 \cos P_h}$ 로 설정하는 단계; 및

제 4원의 반지름을 $\sqrt{d_s^2 + r_1^2 - 2d_s r_1 \cos\left(\frac{P_p}{2} + P_{si}\right)}$ 로 설정하는 단계를 포함하며,

상기 제 1원, 제 2원, 제 3원, 제 4원은 중심점을 공통으로 하고, 상기 결맞음 상태 세트 내 16개의 결맞음 상태는

$$\begin{array}{ll} |\psi_1\rangle &= |r_1 \angle \frac{\pi}{4}\rangle & |\psi_9\rangle &= |r_3 \angle h_0\rangle \\ |\psi_2\rangle &= |r_1 \angle \frac{3\pi}{4}\rangle & |\psi_{10}\rangle &= |r_3 \angle h_1\rangle \\ |\psi_3\rangle &= |r_1 \angle \frac{5\pi}{4}\rangle & |\psi_{11}\rangle &= |r_3 \angle h_2\rangle \\ |\psi_4\rangle &= |r_1 \angle \frac{7\pi}{4}\rangle & |\psi_{12}\rangle &= |r_3 \angle h_3\rangle \\ |\psi_5\rangle &= |r_2 \angle 0\rangle & |\psi_{13}\rangle &= |r_4 \angle g_0\rangle \\ |\psi_6\rangle &= |r_2 \angle \frac{\pi}{2}\rangle & |\psi_{14}\rangle &= |r_4 \angle g_1\rangle \\ |\psi_7\rangle &= |r_2 \angle \pi\rangle & |\psi_{15}\rangle &= |r_4 \angle g_2\rangle \\ |\psi_8\rangle &= |r_2 \angle \frac{3\pi}{2}\rangle & |\psi_{16}\rangle &= |r_4 \angle g_3\rangle \end{array}$$

$$\begin{aligned} r_1 &= \sqrt{2}\alpha \\ r_2 &= (1 + \sqrt{3})\alpha \\ r_3 &= \sqrt{r_2^2 + 2^2 - 4r_2 \cos P_h} \\ r_4 &= \sqrt{d_s^2 + r_1^2 - 2d_s r_1 \cos\left(\frac{P_p}{2} + P_{si}\right)} \\ P_0 &= \tan^{-1}\left(\frac{1}{r_2 - 1}\right) \\ P_{si} &= \pi - \frac{\pi}{4} - P_0 \\ \phi &= 2\pi - 2P_{si} \\ P_p &= \phi - \frac{\pi}{3} \\ b &= \pi - P_p \\ d_s &= \sqrt{8 - 8 \cos b} \\ P_h &= \frac{\pi}{3} + P_0 \end{aligned}$$

$$\begin{aligned} h_0 &= \sin^{-1}\left(\frac{2}{r_3} \sin P_h\right) \\ h_1 &= \pi - h_0 \\ h_2 &= \pi + h_0 \\ h_3 &= -h_0 \\ g_0 &= \frac{\pi}{4} + \sin^{-1}\left(\frac{d_s}{r_4} \sin\left(\frac{P_p}{2} + P_{si}\right)\right) \\ g_1 &= \pi - g_0 \\ g_2 &= \pi + g_0 \\ g_3 &= -g_0 \end{aligned}$$

인 양자 신호 송신 방법.(단, α 는 가변적으로 선택되는 에너지의 크기임)

청구항 4

양자 통신을 위한 양자 수신장치의 양자 신호 검출 방법에 있어서,

양자 송신장치에서 구성된 M배열 원형 직교 진폭 변조(circular QAM) 결맞음 상태 세트를 저장하는 단계; 및
상기 저장된 M 배열 원형 직교 진폭 변조 결맞음 상태 세트에 기초하여, 상기 양자 송신 장치로부터 수신된 결

맞음 상태 $|\psi_i\rangle$ 가 오검출된 결맞음 상태 $|\psi_j\rangle$ 로 검출될 확률을 계산하는 단계를 포함하는 양자 신호 검출 방법.

청구항 5

제 4 항에 있어서,

상기 수신된 결맞음 상태 $|\psi_i\rangle$ 의 평균 광자수 N_s 를 산출하는 단계; 및

상기 산출된 평균 광자수와 상기 계산된 확률 간의 관계를 표시하는 단계를 더 포함하는 양자 신호 검출 방법.

청구항 6

제 4항에 있어서,

상기 계산하는 단계는

진치 행렬, SRM(Square Root Measurement) 측정기, 및 상기 수신된 결맞음 상태 $|\psi_i\rangle$ 에 대한 양자 상태 값 간의 연산을 통해 계산하고,

상기 SRM 측정기는

$$\hat{G} = \sum_{i=1}^M |\psi_i\rangle \langle \psi_i|$$
 및 상기 오검출된 결맞음 상태 $|\psi_j\rangle$ 에 대한 양자 상태 값을 기초로 산출된 $|\mu_j\rangle$ 에 대한 양자 상태 값으로 정의되는 것인, 양자 신호 검출 방법.

발명의 설명

기술 분야

[0001] 본 발명은 양자 통신을 위한 시스템 및 양자 신호 송수신 방법에 관한 것이다.

배경 기술

[0002] 1984년 C. H. Bennett과 G. Brassard에 의해 고안된 BB84 QKD 프로토콜이 알려진 이후, 지난 20년간 양자암호 분야에 엄청난 발전해왔다. 양자 키 분배(Quantum Key Distribution) 프로토콜의 핵심은 멀리 떨어져 있는 두 사용자가 암호 통신을 위한 비밀 키를 생성 및 공유함과 동시에 공유된 비밀 키에 대한 무조건적 안전성(Unconditional Security)을 보장하여 공개된 통신 채널을 통해 통신하는 것이다.

[0003] 양자 키 분배 프로토콜은 현재 가장 안전한 최신 암호 통신 기술로서, 사용자 사이에서 교환되는 암호를 가로채는 맨 인 더 미들(Man-in-the-middle) 공격에 대한 안전성을 보장하기 위하여 사용자에게 대한 인증방식을 요구하고 있다. 가장 대표적으로 사용되는 인증방식은 고전 암호 인증방식과 양자 키 분배 인증방식을 결합하는 것이다.

[0004] 그러나 고전 암호 인증방식을 적용하지 않고 양자적 성질만을 이용한 양자 키 분배 인증 방식은 존재하지 않으며, 또한 양자 키 분배 프로토콜 이외의 다자간 양자 암호 통신 프로토콜의 경우에 있어서는 아직 사용자 인증 방식이 연구되고 있지 못한 상황이다.

[0005] 양자 암호 통신에 있어 양자 상태는 복제가 불가능하여 그에 따라 필연적 검출 오류 확률이 존재하게 되고, 결국 필연적 오류확률로 인해 확실성을 가지고 검출하는 것이 불가능하기 때문이다.

[0006] 따라서 이러한 문제를 해결하기 위해서, 양자 송신장치가 M개의 양자 상태 중 임의의 하나를 골라 양자 수신장치로 보내고, 수신장치가 송신장치가 보낸 양자 상태를 측정하여 검출하는 방법에 대하여 다양한 방법이 연구되고 있다. 아래는 그에 따른 연구들이다.

[0007] M. Ban, K. Kurokawa, R. Momose, and O. Hirota, "Optimum measurements for Discrimination among Symmetric Quantum states and parameter estimation," International Journal of Theoretical Physics, vol. 36, no. 6, pp. 1269.1288, 1997.에서는 위상 편이 방식 형태의 양자 상태를 구별하기 위한 측정으로 SRM(Square Root Measurement) 기법을 제안하였으며, 해당 측정 기법이 측정 오류 측면에서 최적의 방식임을 증명하였다.

[0008] K. Kato, M. Osaki, M. Sasaki, and O. Hirota, "Quantum detection and Mutual information for QAM and

PSK signals,” Communications, IEEE Transactions on, vol. 47, no. 2, pp. 248.254, 1999.에서는 직교 진폭 변복조 형태의 상태를 구별하기 위한 측정으로 Square Root Measurement(SRM)을 이용할 것을 제안하였고, 비록 그것이 최적의 방식임을 증명하지는 못했지만 위상 편이 방식에 비하여 오히려 더 좋은 측정 성능을 갖는 방식을 증명하였다.

발명의 내용

해결하려는 과제

- [0009] 본 발명의 일부 실시예는 양자 상태의 성질만을 이용한 인증 방식으로 상대방과 비밀 키 공유하여 통신하는 양자 통신 시스템에서의 양자 송수신 장치의 양자 신호 송수신 방법을 제공하는 것을 그 목적으로 한다.
- [0010] 다만, 본 실시예가 이루고자 하는 기술적 과제는 상기된 바와 같은 기술적 과제로 한정되지 않으며, 또 다른 기술적 과제들이 존재할 수 있다.

과제의 해결 수단

- [0011] 상술한 기술적 과제를 달성하기 위한 기술적 수단으로서, 본 발명의 일 실시예에 따른 양자 통신을 위한 양자 송신 장치의 양자 신호 송신 방법은, M배열 원형 직교 진폭 변조(Circular QAM) 결맞음 상태 세트를 구성하는 단계, 송신하고자 하는 메시지에 따라 결맞음 상태 세트 내 M개의 결맞음 상태 중 어느 하나를 선택하는 단계 및 결맞음 상태 세트를 공유하는 양자 수신장치로 선택된 결맞음 상태를 송신하는 단계를 포함하고, 상기 구성하는 단계는 가변적으로 선택되는 에너지 내에서 결맞음 상태간 최소 유클리드 거리가 최대화 되도록 구성한다.
- [0012] 또한, 본 발명의 일 실시예에 따른 양자 통신을 위한 양자 수신장치의 양자 신호 검출 방법은 양자 송신장치에서 구성된 M배열 원형 직교 진폭 변조 (Circular QAM) 결맞음 상태 세트를 저장하는 단계 및 양자 송신 장치로부터 수신된 결맞음 상태 $|\psi_i\rangle$ 가 오검출된 결맞음 상태 $|\psi_j\rangle$ 로 검출될 확률을 계산하는 단계를 포함한다.

발명의 효과

- [0013] 전술한 본 발명의 과제 해결 수단 중 어느 하나에 의하면, 최소 거리를 갖는 원형 직교 진폭 변조를 통해 양자 결맞음 상태 세트를 구성함으로써, 동일한 광자수에 대하여 종래 기법들보다 양자 신호 검출의 오류 확률을 저감시킬 수 있다.

도면의 간단한 설명

- [0014] 도 1은 본 발명의 실시 예에 따른 양자 통신 시스템의 구조가 도시된 도면이다.
- 도 2는 16 배열 사각형 직교 진폭 변조(Rectangular QAM)에 따른 결맞음 상태 세트를 도시한 도면이다.
- 도 3은 도 1에 도시된 양자 송신 장치의 양자 전송 과정에 대한 흐름을 나타낸 도면이다.
- 도 4는 8 배열 원형 직교 진폭 변조시 최소 유클리드 거리를 최대화하는 결맞음 상태 세트를 나타낸 도면이다.
- 도 5는 16 배열 원형 직교 진폭 변조시 최소 유클리드 거리를 최대화하는 결맞음 상태 세트를 나타낸 도면이다.
- 도 6은 도 1에 도시된 양자 수신장치의 양자 신호 검출 과정에 대한 흐름을 나타낸 도면이다.
- 도 7은 본 발명의 실시예에 따른 성능을 그래프로 나타낸 도면이다.

발명을 실시하기 위한 구체적인 내용

- [0015] 아래에서는 첨부한 도면을 참조하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 본 발명의 실시 예를 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시 예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.
- [0016] 명세서 전체에서, 어떤 부분이 다른 부분과 "연결"되어 있다고 할 때, 이는 "직접적으로 연결"되어 있는 경우뿐 아니라, 그 중간에 다른 소자를 사이에 두고 "전기적으로 연결"되어 있는 경우도 포함한다. 또한 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아

니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다.

- [0017] 도 1은 본 발명의 실시 예에 따른 양자 통신 시스템의 구조가 도시된 도면이다.
- [0018] 도 1에 도시된 바와 같이, 본 발명의 실시 예에 따른 양자 통신 시스템은 양자 생성부(112) 및 양자 전송부(114)를 포함한 양자 송신장치(100)와 양자 검출부(122) 및 오류 산출부(124)를 포함한 양자 수신장치(120)로 구성되며, 양자 송수신 장치는 양자 채널(130)을 통해 연결된다.
- [0019] 다만 이러한 도 1의 양자 통신 시스템은 본 발명의 실시 예에 불과함으로 도 1을 통해 본 발명이 한정적으로 해석되는 것은 아니다. 즉, 본 발명의 다양한 실시 예들에 따르면, 양자 통신 시스템은 도 1과 다르게 구성될 수 있다.
- [0020] 양자 송신장치(100)와 양자 수신장치(120)는 일반적으로 양자 채널(130)을 통해 연결되는데, 양자 채널(130)은 예를 들어 상용 광통신 망에 약화시킨 레이저를 통해 구현될 수 있다.
- [0021] 양자 송신장치(100)는 양자 생성부(112)와 양자 전송부(114)를 포함한다.
- [0022] 양자 생성부(112)는 소정의 정보가 양자 통신에 의해 적합하게 전송될 수 있도록 결맞음 상태 세트를 생성한다. 예를 들면 양자 결맞음 상태 세트는 8 배열 또는 16 배열 사각형 직교 진폭 변조(Rectangular QAM) 혹은 8 배열 또는 16 배열 원형 직교 진폭 변조 (Circular QAM) 등과 같은 다양한 배열 및 변조 방식에 의해 구성될 수 있다.
- [0023] 일반적으로 M배열 양자 결맞음 상태 세트는 힐버트 공간(Hilbert space)에서 M개의 순수 상태(Pure State)로 나타낼 수 있다. 각각의 상태는 트레이스(Trace) 값이 1이고, 양반한정행렬(Positive Semi Definite Matrix)인 상태 밀도 연산(Density Operator)으로 표현할 수 있다. 또한 순수 상태(Pure State)이므로 각각의 상태 밀도 연산(Density Operator)은 벡터 형식으로 나타낼 수 있으며, 결맞음 상태 각각을 $|\psi_i\rangle$ ($i=1,2,\dots,M$)로 표현할 수 있다.
- [0024] 양자 전송부(114)는 송신하려는 정보에 따라 양자 생성부(112)에서 생성된 결맞음 상태 세트 중 사용자에게 의해 선택된 결맞음 상태를 양자 수신장치(120)로 전송한다.
- [0025] 이때, 양자 송신장치(100)와 양자 수신장치(120)는 결맞음 상태 세트를 서로 공유한다.
- [0026] 양자 수신장치(120)는 양자 검출부(122)와 오류 산출부(124)를 포함한다.
- [0027] 양자 검출부(122)는 SRM(Square Root Measurement)검출기를 사용하여 수신된 양자 결맞음 상태를 검출한다.
- [0028] 오류 산출부(124)는 수신된 양자 결맞음 상태가 다른 결맞음 상태로 오검출될 확률을 산출한다. 이때, 수신된 결맞음 상태 $|\psi_i\rangle$ 의 평균 광자수와 오검출될 확률 간의 관계가 양자 수신장치(120)에 포함되거나 양자 수신장치(120)와 연결된 표시장치(미도시)에 표시될 수 있다.
- [0029] 도 2는 16 배열 사각형 직교 진폭 변조(Rectangular QAM)에 따른 결맞음 상태 세트를 도시한 도면이다.
- [0030] 도 2는 Kato의 논문에서 제시하고 있는 양자 상태 변조 방법으로 16 배열 사각형 직교 진폭 변조(Rectangular QAM)에 따른 결맞음 상태 세트 예시이다.
- [0031] Kato의 연구에 따르면 양자 신호 전송에 있어, PSK(Phase Shift Keying) 변조방식이 아닌 QAM(Quadrature Amplitude Modulation)을 제안하였고, 소멸연산자(Annihilation Operator)와 생성연산자(Creation Operator)의 선형 조합으로 결맞음 상태 세트를 구성한다.
- [0032] 소멸연산자(Annihilation Operator)는 양자 단일 조화 진동자에서 주어진 상태 준위를 한 단계 낮추는 연산자이다. 생성연산자(Creation Operator)는 소멸연산자(Annihilation Operator)의 복소 켤레(Complex Conjugate)이다.
- [0033] 도 2의 d1 및 d2를 살펴보면, kato는 최소거리에 해당하는 2α 에 따라 16개의 양자 결맞음 상태를 구성하였으며, X좌표와 같이 결맞음 상태를 $|(3-i)\alpha\rangle$ 로 표현할 수 있다.

- [0034] 이 표현 방식은 폴 디랙의 방정식에 따른다. 폴 디랙은 양자역학과 특수 상대성 이론을 통합하여 디랙 방정식을 만들었고, 브라켓 기호를 이용한 연산자 이론을 최초로 사용했다. 예를 들어 브라켓 노테이션에서, $\langle A|$ 는 브라 A 이고, $|A\rangle$ 는 켓 A 이다. 이때 $|A\rangle$ 는 컬럼 벡터이고, $\langle A|$ 는 $|A\rangle$ 의 에르미트 행렬(Hermitian)이다.
- [0035] 본 발명의 일 실시예는 도 2의 Kato의 연구의 발전형으로 수신된 결맞음 상태의 측정 성능이 각 상태들 사이의 최소 유클리드 거리에 영향을 받는다는 사실에 착안하였으며, M배열 원형 직교 진폭 변조(Circular QAM) 결맞음 세트 구성시 최소 유클리드 거리를 최대화할 수 있는 상태의 조합을 제안한다.
- [0036] 최소 유클리드 거리를 최대화하는 양자 상태를 설명하기 위한 간단한 예를 들면 양자 상태들이 다음과 같이 gap과 을로 구성되어 있다고 한다면, gap: $[-3, -1, 1, 3]$ 을: $[-5, -4, 1, 3]$ 일 때, 을의 경우 gap에 비해 전반적으로 양자 상태가 더 멀리 떨어져 있지만 $[-5]$ 와 $[-4]$ 가 너무 가까워서 최소 유클리드 거리가 1이 되는 상황이다. 이런 상황을 피해서 gap처럼 구성하는 것이 최소 유클리드 거리를 최대화하는 것이다.
- [0037] 도 2를 참조하여 또 다른 예를 들면, 가변적으로 선택되는 에너지 내에 존재할 수 있는 광자수는 한정적이고, 성장도의 바깥쪽에 결맞음 상태가 위치할수록 많은 광자 수를 갖게 된다. 따라서 한정된 광자 수 내에서 양자 상태들을 최대한 멀리 떨어뜨려 놓는 것이 최소 유클리드 거리를 최대화하는 것이다.
- [0038] 양자의 결맞음 상태 간 유클리드 거리를 최대화하는 이유에 대하여 [수학식 1] 내지 [수학식 6]을 통해 자세히 설명하도록 한다.
- [0039] 한편, 도 3은 도 1에 도시된 양자 송신 장치의 양자 전송 과정에 대한 흐름을 나타낸 도면이다.
- [0040] 본 발명의 실시예에 따른 양자 통신을 위한 양자 송신장치(100)의 양자 신호 송신방법은, 양자 송신장치(100)를 통해 M배열 원형 직교 진폭 변조(Circular QAM) 결맞음 상태 세트를 구성한다(S300).
- [0041] 다음으로, 양자 송신장치(100)는 송신하려는 메시지에 따라 결맞음 상태 세트 내 M개의 결맞음 상태 중 어느 하나를 선택한다(S310).
- [0042] 다음으로, 양자 송신장치(100)는 결맞음 상태 세트를 공유하는 양자 수신장치(120)로 상기 선택된 결맞음 상태를 송신한다(S320).
- [0043] 도 4는 8 배열 원형 직교 진폭 변조시 최소 유클리드 거리를 최대화하는 결맞음 상태 세트를 나타낸 도면이다.
- [0044] 양자 생성부(112)는 8 배열 원형 직교 진폭 변조 결맞음 상태 세트 생성시, 최소 유클리드 거리가 2α 일 때, 제 1원의 반지름을 $\sqrt{2}\alpha$ 로 설정하고, 제 1원과 중심점을 공유하는 제 2원의 반지름을 $(1 + \sqrt{3})\alpha$ 로 설정할 수 있다.
- [0045] 이때, 각 결맞음 상태 세트의 좌표를 알고 있기 때문에, 피타고라스 정리에 의해서 유클리드 거리가 구해질 수 있다.
- [0046] 이때, 최소거리 2α 에 따른 8 배열 원형 직교 진폭 변조 결맞음 상태 세트의 구성은 아래와 같이 나타낼 수 있다.
- $$\begin{aligned} |\psi_1\rangle &= |\alpha(1 + j)\rangle \\ |\psi_2\rangle &= |\alpha(-1 + j)\rangle \\ |\psi_3\rangle &= |\alpha(-1 - j)\rangle \\ |\psi_4\rangle &= |\alpha(1 - j)\rangle \\ |\psi_5\rangle &= |\alpha(1 + \sqrt{3})\rangle \\ |\psi_6\rangle &= |\alpha j(1 + \sqrt{3})\rangle \\ |\psi_7\rangle &= |-\alpha(1 + \sqrt{3})\rangle \\ |\psi_8\rangle &= |-\alpha j(1 + \sqrt{3})\rangle \end{aligned}$$
- [0047]
- [0048] 도 5는 16 배열 원형 직교 진폭 변조시 최소 유클리드 거리를 최대화하는 결맞음 상태 세트를 나타낸 도면이다.
- [0049] 양자 생성부(112)에서 16 배열 양자 직교 진폭 변조 결맞음 상태 세트 구성시, 결맞음 상태간 최소 유클리드 거

리가 2α 일때, 중심점을 공통으로 한 제 1원, 제 2원, 제 3원, 제 4원을 다음과 같이 설정할 수 있다.

[0050] 이때, 제 1원의 반지름을 $\sqrt{2}\alpha$ 로 설정하고, 제 2원의 반지름을 $(1+\sqrt{3})\alpha$ 로, 제 3원의 반지름을 $\sqrt{r_2^2 + 2^2 - 4r_2 \cos P_h}$ 로, 제 4원의 반지름을 $\sqrt{d_s^2 + r_1^2 - 2d_s r_1 \cos\left(\frac{P_p}{2} + P_{si}\right)}$ 로 설정할 수 있다.

[0051] 이때, 각 결맞음 상태 세트의 좌표를 알고 있기 때문에 피타고라스 정리에 의해서 유클리드 거리를 구할 수 있고, 이에 따라 세트 $|\psi_i\rangle$ ($i=1,2,\dots,M$)로 표현되는 16개의 결맞음 상태를 구할 수 있다.

[0052] 최소거리 2α 에 따른 16 배열 원형 직교 진폭 변조 결맞음 상태 세트의 구성은 아래와 같이 나타낼 수 있다.

$$\begin{array}{ll} |\psi_1\rangle = |r_1 \angle \frac{\pi}{4}\rangle & |\psi_9\rangle = |r_3 \angle h_0\rangle \\ |\psi_2\rangle = |r_1 \angle \frac{3\pi}{4}\rangle & |\psi_{10}\rangle = |r_3 \angle h_1\rangle \\ |\psi_3\rangle = |r_1 \angle \frac{5\pi}{4}\rangle & |\psi_{11}\rangle = |r_3 \angle h_2\rangle \\ |\psi_4\rangle = |r_1 \angle \frac{7\pi}{4}\rangle & |\psi_{12}\rangle = |r_3 \angle h_3\rangle \\ |\psi_5\rangle = |r_2 \angle 0\rangle & |\psi_{13}\rangle = |r_4 \angle g_0\rangle \\ |\psi_6\rangle = |r_2 \angle \frac{\pi}{2}\rangle & |\psi_{14}\rangle = |r_4 \angle g_1\rangle \\ |\psi_7\rangle = |r_2 \angle \pi\rangle & |\psi_{15}\rangle = |r_4 \angle g_2\rangle \\ |\psi_8\rangle = |r_2 \angle \frac{3\pi}{2}\rangle & |\psi_{16}\rangle = |r_4 \angle g_3\rangle \end{array}$$

[0053] 다음의 변수들에 의해서 결맞음 상태 세트를 각각 계산할 수 있다.

[0054]

$$\begin{array}{ll} r_1 &= \sqrt{2}\alpha \\ r_2 &= (1+\sqrt{3})\alpha \\ r_3 &= \sqrt{r_2^2 + 2^2 - 4r_2 \cos P_h} \\ r_4 &= \sqrt{d_s^2 + r_1^2 - 2d_s r_1 \cos\left(\frac{P_p}{2} + P_{si}\right)} \\ P_0 &= \tan^{-1}\left(\frac{1}{r_2 - 1}\right) \\ P_{si} &= \pi - \frac{\pi}{4} - P_0 \\ \phi &= 2\pi - 2P_{si} \\ P_p &= \phi - \frac{\pi}{3} \\ b &= \pi - P_p \\ d_s &= \sqrt{8 - 8 \cos b} \\ P_h &= \frac{\pi}{3} + P_0 \end{array}$$

[0055]

$$\begin{array}{ll} h_0 &= \sin^{-1}\left(\frac{2}{r_3} \sin P_h\right) \\ h_1 &= \pi - h_0 \\ h_2 &= \pi + h_0 \\ h_3 &= -h_0 \\ g_0 &= \frac{\pi}{4} + \sin^{-1}\left(\frac{d_s}{r_4} \sin\left(\frac{P_p}{2} + P_{si}\right)\right) \\ g_1 &= \pi - g_0 \\ g_2 &= \pi + g_0 \\ g_3 &= -g_0. \end{array}$$

[0056] 아울러, 도 6은 도 1에 도시된 양자 수신장치의 양자 신호 검출 과정에 대한 흐름을 나타낸 도면이다.

[0057]

[0058] 본 발명의 실시예에 따른 양자 통신을 위한 양자 수신장치의 양자 신호 검출방법은 먼저 양자 수신장치의 양자 송신장치에서 구성된 M배열 원형 직교 진폭 변조 (circular QAM) 결맞음 상태 세트를 저장한다(S600).

[0059] 다음으로 양자 수신장치는 SRM(Square Root Measurement) 검출기를 사용하여 수신된 양자 신호를 검출한다(S610).

[0060] 다음으로, 양자 수신장치는 양자 송신 장치로부터 수신된 결맞음 상태 $|\psi_i\rangle$ 가 오검출된 결맞음 상태 $|\psi_j\rangle$ 로 검출될 확률 $P(j|i) = \text{Tr} \hat{\Pi}_j \rho_i$ 을 계산한다(S620).

[0061] 여기서, Tr은 전치행렬(Transpose matrix) 연산이며, ρ_i 는 수신장치에서 얻을 수 있는 양자 상태(Quantum state) 값으로 수신된 결맞음 상태와 수신장치에서 알고 있는 결맞음 상태 $|\psi_i\rangle$ 의 브라켓 연산을 통해서 얻을 수 있다.

[0062] 즉 양자 수신장치(120)는 양자 송신장치(100)로부터 수신된 결맞음 상태 $|\psi_i\rangle$ 와 미리 공유하고 있는 결맞음 상태에 $|\psi_i\rangle$ 대한 브라켓 연산을 수행한 후 얻은 ρ_i 과 측정기 $\hat{\Pi}_j$ 과의 전치행렬을 연산하면 오검출 확률을 구할 수 있다.

[0063] 양자 검출부(122)에서 수신된 결맞음 상태 오검출을 위해 사용하는 SRM(Square Root Measurement) 측정기 $\hat{\Pi}_j$ 는 [수학식 1] 내지 [수학식 4]를 통해 구할 수 있다.

수학식 1

$$\hat{G} = \sum_{i=1}^M |\psi_i\rangle \langle \psi_i|$$

[0064]

수학식 2

$$|\mu_j\rangle = \hat{G}^{-1/2} |\psi_j\rangle$$

[0065]

수학식 3

$$\hat{\Pi}_j = |\mu_j\rangle \langle \mu_j|$$

[0066]

[수학식 1]의 $|\psi_i\rangle$ 는 i번째 결맞음 상태이며, 양자 송신장치(100)와 양자 수신장치(120)가 수신자가 공유하고 있는 결맞음 상태 세트 중 하나로 브라켓 연산을 하여 얻어진 행렬들을 더해서 $\hat{G}$ 를 구할 수 있다.

[0068] [수학식 2]에서 $|\mu_j\rangle$ 를 구하기 위해서 $\hat{G}^{-1/2}$ 값이 필요한데, $\hat{G}$ 의 역행렬을 H라 하면 H를 고유값 분해 통해 $H=USU^T$ 로 나타낼 수 있으며, S의 각 항의 양의 제곱근을 대각항으로 가지는 행렬을 R이라 했을 때 $H^{-1/2}=URU^T$ 로

구할 수 있다. 이를 통해 구해진 $\hat{G}^{-1/2}$ 과 $|\psi_j\rangle$ 의 연산을 통해 $|\mu_j\rangle$ 를 구할 수 있다.

[0069] [수학식 3]에서는 [수학식 2]를 통하여 구해진 $|\mu_j\rangle$ 과 $\langle\mu_j|$ 의 브라켓 연산을 통해 i번째 신호가 왔음을 검출할 수 있는 SRM(Square Root Measurement) 측정기 $\hat{\Pi}_j$ 를 구할 수 있다.

[0070] SRM(Square Root Measurement)측정기를 이용해서 검출을 할 때 검출 성능을 구하는 과정에서 G (Gram matrix)를 사용하게 되는데, 아래의 [수학식 4]와 같다.

수학식 4

[0071]

$$G = \begin{bmatrix} \langle\psi_1|\psi_1\rangle & \cdots & \langle\psi_1|\psi_M\rangle \\ \vdots & \ddots & \vdots \\ \langle\psi_M|\psi_1\rangle & \cdots & \langle\psi_M|\psi_M\rangle \end{bmatrix}$$

[0072] G (Gram matrix)의 i행 j열은 i번째 상태와 j번째 상태의 내적으로, 각 성분이 두 결맞음 상태 사이의 내적으로 이루어져 있다.

[0073] [수학식 5] 내지 [수학식 6]은 두 결맞음 상태 사이의 내적을 구한 식이다.

수학식 5

[0074]

$$\begin{aligned} \langle\alpha|\beta\rangle &= e^{-\frac{|\alpha|^2+|\beta|^2}{2}} \sum_{m=0}^{\infty} \sum_{n=0}^{\infty} \frac{\alpha^{*m}\beta^n}{\sqrt{m!n!}} \langle m|n\rangle \\ &= e^{-\frac{|\alpha|^2+|\beta|^2}{2}} \sum_{n=0}^{\infty} \frac{(\alpha^*\beta)^n}{n!} \\ &= e^{-\frac{|\alpha|^2+|\beta|^2}{2}+\alpha^*\beta} \\ &= A_{\alpha\beta} \exp j\theta_{\alpha\beta} \end{aligned}$$

수학식 6

[0075]

$$\begin{aligned} A_{\alpha\beta} &= \exp \left[-\frac{\alpha^2}{2} ((\alpha_R - \beta_R)^2 + (\alpha_I - \beta_I)^2) \right] \\ \theta_{\alpha\beta} &= [\alpha^2(\alpha_R\beta_I - \alpha_I\beta_R)]. \end{aligned}$$

[0076] [수학식 6]은 [수학식 5]에서 구한 내적을 복소수를 크기 $A_{\alpha\beta}$ 와 편각 $\exp j\theta_{\alpha\beta}$ 로 표현한 것으로 알파와 베타가 다른 경우(비대각항) 그 값의 크기가 작아야 오류율이 낮아짐을 알 수 있다.

[0077] 즉, 본 발명의 실시예에서 양자의 결맞음 상태 간 유클리드 거리를 최대화하는 이유는 각 상태간 유클리드 거리가 작을 때 오류율이 작기 때문이다.

[0078] 도 7은 본 발명의 실시예에 따른 성능을 그래프로 나타낸 도면이다.

[0079] 비교의 대상이 되는 세로축은 검출 에러 확률(Detection error rate)이며, 가로축은 결맞음 상태의 평균 광자 숫자이다. 이는 고전 디지털 통신에서 동일 SNR(Signal to Noise Ratio)에서 더 낮은 오류확률을 비교하는 것과 동일하다.

[0080] [수학식 7]은 도 7의 그래프의 가로축인 결맞음 상태의 평균 광자 숫자를 구하는 식이다.

수학식 7

$$N_s = \sum_{i=1}^M q_i \langle \psi_i | \hat{n} | \psi_i \rangle$$

[0081]

[0082] $\hat{n} = \hat{a}^\dagger \hat{a}$ 는 넘버 연산(Number Operator)으로 양자 상태의 연산중 하나이로 행렬로 나타낼 수 있으며, 이는 고전 디지털 통신에서의 어떤 ‘시스템’ 이라고 할 수 있다.

[0083] $|\psi_i\rangle$ 는 송신 장치와 수신 장치가 준비하는 M개의 결맞음 상태 세트중의 i번째 상태를 나타낸다. 이때, 각 상태들은 칼럼 벡터로 나타낼 수 있다.

[0084] $\langle \psi_i |$ 는 $|\psi_i\rangle$ 의 에르미트 행렬(Hermitian)로 벡터이며, $\langle \psi_i |$ 과 $|\psi_i\rangle$ 의 넘버 연산(number operator)을 하면 실수값을 구할 수 있다. 이때 이 실수값은 i 번째 상태의 광자수를 의미하며, 고전 디지털 통신에서의 i 번째 신호의 신호 에너지와 유사하다.

[0085] 넘버 연산후 1부터 M개의 결맞음 상태에 대해 각각의 선험적 확률 q_i (Priori Probability)을 곱한 후 더하여 전체 양자 상태 세트의 평균 광자 수 N_s 를 구할 수 있다.

[0086] 도 7의 굵은 원형 단추로 표시한 것이 본 발명의 실시 예인 원형 직교 진폭 변조(Circular QAM)에 따른 측정 오류 성능이고 가는 사각 단추로 표시한 것이 Kato의 연구 성과의 성능이다.

[0087] 도 7의 A는 8 배열 원형 직교 진폭 변조(Circular QAM) 과 Kato의 8 배열 사각형 직교 진폭 변조(Rectangular QAM)의 성능을 비교하고 있다.

[0088] 검출 에러 확률이 10^{-3} 일 때 각각의 변조방식에 대한 광자수를 비교하고 있으며, 본 발명의 일 실시예인 8 배열 원형 직교 진폭 변조(Circular QAM)가 Kato의 8 배열 사각형 직교 진폭 변조(Rectangular QAM)보다 더 적은 광자수로도 동일한 검출 에러 확률을 얻음을 확인할 수 있다.

[0089] 도 7의 B는 16 배열 원형 직교 진폭 변조(Circular QAM) 과 Kato의 16 배열 사각형 직교 진폭 변조(Rectangular QAM)의 성능을 비교하고 있다.

[0090] 검출 에러 확률이 10^{-3} 일 때 각각의 변조방식에 대한 광자수를 비교하고 있으며, 본 발명의 다른 실시예인 16 배열 원형 직교 진폭 변조(Circular QAM)가 Kato의 16 배열 사각형 직교 진폭 변조(Rectangular QAM)보다 더 적은 광자수로도 동일한 검출 에러 확률을 얻음을 확인할 수 있다.

[0091] 진술한 본 발명의 설명은 예시를 위한 것이며, 본 발명이 속하는 기술분야의 통상의 지식을 가진 자는 본 발명의 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 쉽게 변형이 가능하다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시 예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 예를 들어, 단일형으로 설명되어 있는 각 구성 요소는 분산되어 실시될 수도 있으며, 마찬가지로

지로 분산된 것으로 설명되어 있는 구성 요소들도 결합된 형태로 실시될 수 있다.

[0092]

본 발명의 범위는 상기 상세한 설명보다는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

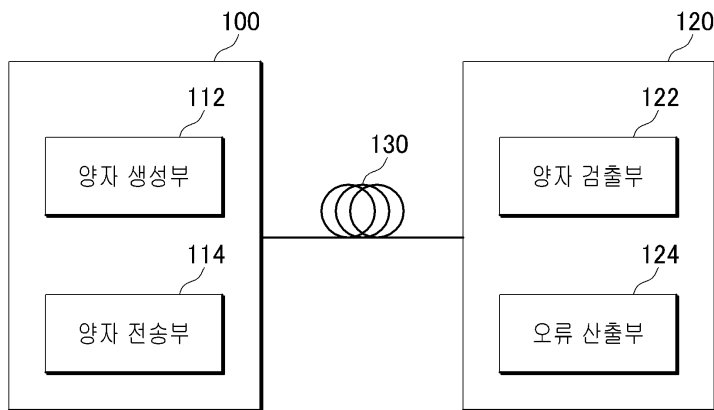
부호의 설명

[0093]

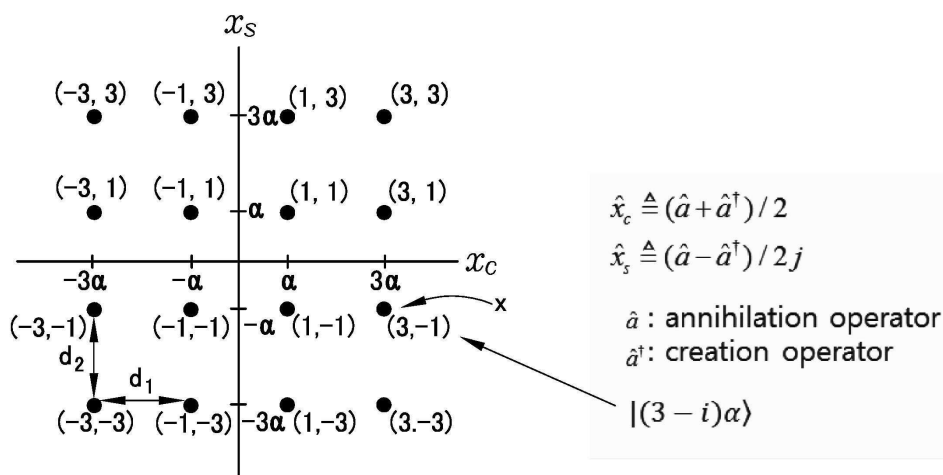
100: 양자 송신장치	112: 양자 생성부
114: 양자 전송부	120: 양자 수신장치
122: 양자 검출부	124: 오류 산출부
130: 양자 채널	

도면

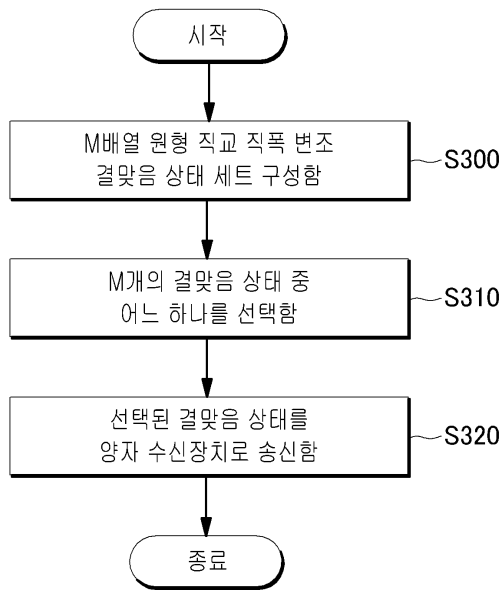
도면1



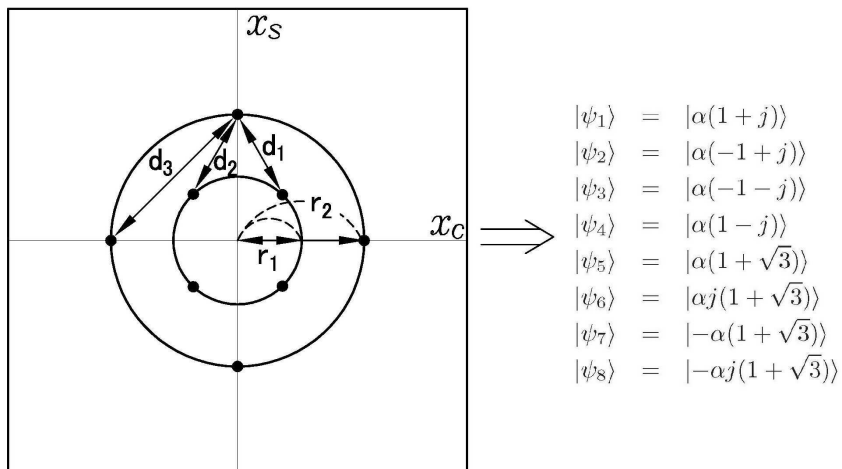
도면2



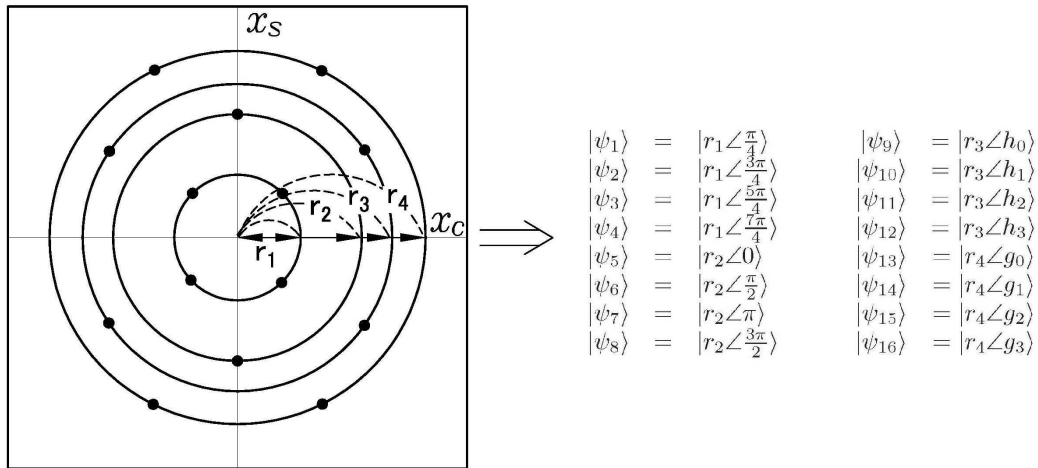
도면3



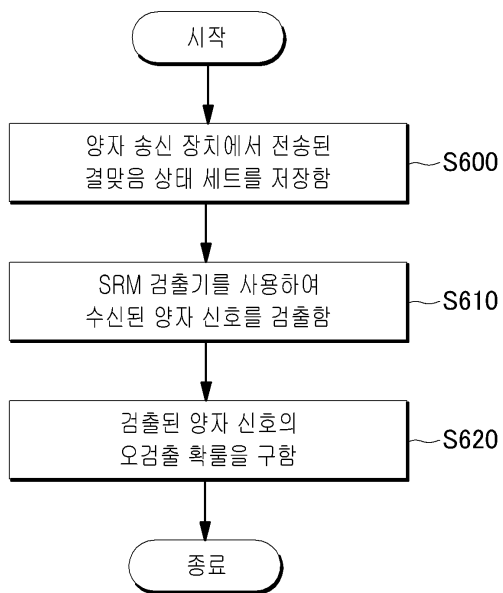
도면4



도면5



도면6



도면7

