(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0022594
(43) 공개일자 2020년03월04일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *H04L 7/00* (2006.01)
(52) CPC특허분류
H04L 9/0819 (2013.01)
H04L 7/0008 (2013.01)
(21) 출원번호 10-2018-0098369
(22) 출원일자 2018년08월23일
심사청구일자 2018년08월23일

(71) 출원인
인천대학교 산학협력단
인천광역시 연수구 아카데미로 119 (송도동)
(72) 발명자
유용석
인천광역시 연수구 아카데미로 119 (송도동, 인천대학교)
(74) 대리인
특허법인충정

전체 청구항 수 : 총 10 항

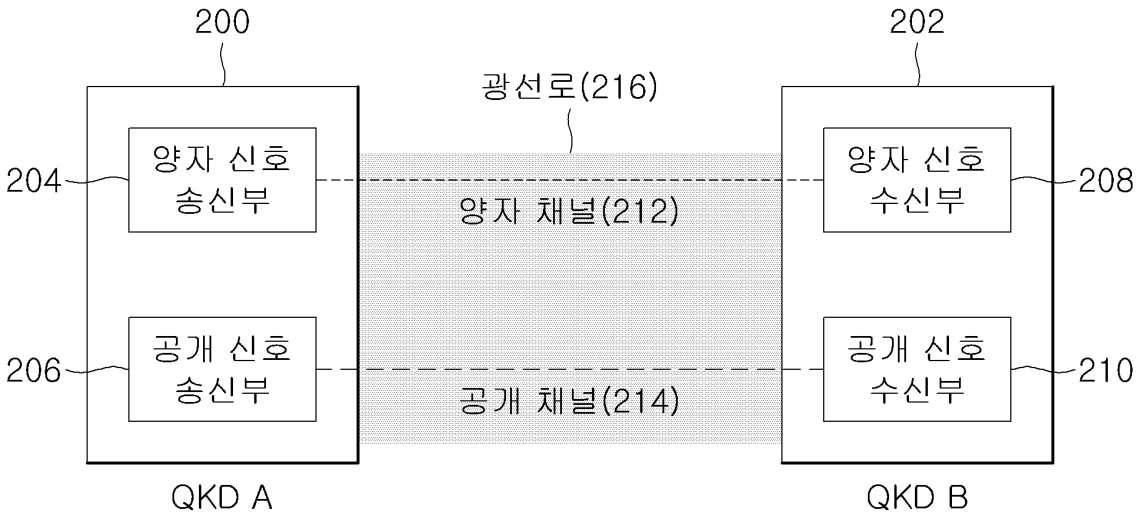
(54) 발명의 명칭 **단일 링크 기반 양자 키 분배 시스템 및 방법**

(57) 요 약

본 발명의 일 실시예에 의한 단일 링크 기반 양자 키 분배 시스템은, 양자 채널을 통해 양자 키와 관련된 양자 신호를 송신하기 위한 양자 신호 송신부 및 공개 채널을 통해 양자 신호를 처리하기 위한 동기화 신호 및 관리 신호를 포함하는 공개 신호를 송신하기 위한 공개 신호 송신부를 포함하는 양자 키 분배 송신부; 및 상기 양자

(뒷면에 계속)

대 표 도 - 도2



신호 송신부에서 송신하는 양자 신호를 상기 양자 채널을 통해 수신하여 상기 양자 키를 검출하기 위한 양자 신호 수신부 및 상기 공개 신호 송신부에서 송신하는 공개 신호를 상기 공개 채널을 통해 수신하기 위한 공개 신호 수신부를 포함하는 양자 키 분배 수신부를 포함하고, 상기 양자 채널과 상기 공개 채널은 단일 링크로 형성되어, 다양한 구성과 형태의 상용 통신망을 활용한 양자 키 분배 시스템을 가능하게 하여 망 구축 비용 및 유지 보수 비용을 절감하고 시장의 규모를 확대하여 운영자의 이윤을 보장하면서 많은 사용자들에게 암호 키를 제공할 수 있다.

(52) CPC특허분류
H04L 7/0075 (2013.01)
H04L 9/0852 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711058794
부처명 과학기술정보통신부
연구관리전문기관 정보통신기술진흥센터
연구사업명 정보통신방송표준개발지원
연구과제명 양자암호통신 분야 QKD 기술 표준개발
기 여 율 1/1
주관기관 퀀텀정보통신연구조합
연구기간 2017.09.01 ~ 2018.08.31

명 세 서

청구범위

청구항 1

양자 채널을 통해 양자 키와 관련된 양자 신호를 송신하기 위한 양자 신호 송신부 및 공개 채널을 통해 양자 신호를 처리하기 위한 동기화 신호 및 관리 신호를 포함하는 공개 신호를 송신하기 위한 공개 신호 송신부를 포함하는 양자 키 분배 송신부; 및

상기 양자 신호 송신부에서 송신하는 양자 신호를 상기 양자 채널을 통해 수신하여 상기 양자 키를 검출하기 위한 양자 신호 수신부 및 상기 공개 신호 송신부에서 송신하는 공개 신호를 상기 공개 채널을 통해 수신하기 위한 공개 신호 수신부를 포함하는 양자 키 분배 수신부를 포함하고,

상기 양자 채널과 상기 공개 채널은 단일 링크로 형성되는, 단일 링크 기반 양자 키 분배 시스템.

청구항 2

청구항 1에 있어서,

상기 양자 키 분배 수신부는,

상기 양자 채널을 통해 수신되는 양자 수신 신호와 상기 공개 채널을 통해 수신되는 공개 수신 신호를 측정하고,

상기 측정된 공개 수신 신호에 기반하여 상기 공개 신호 송신부에서 송신하는 공개 송신 신호를 예측하며,

상기 측정된 양자 수신 신호와 상기 예측된 공개 송신 신호에 기반하여 상기 양자 신호 송신부에서 송신한 양자 송신 신호를 예측하고,

상기 예측된 양자 송신 신호에 기반하여 상기 양자 키를 검출하는, 단일 링크 기반 양자 키 분배 시스템.

청구항 3

청구항 2에 있어서,

상기 양자 키 분배 수신부는,

수학식 1에 기반하여 상기 양자 신호 송신부에서 송신한 양자 송신 신호(X_1)를 예측하고,

[수학식 1]

$$Y_1 = aX_1 + bX_2 + Z_1$$

$$Y_2 = cX_2 + Z_2$$

Y_1은 상기 양자 채널을 통해 수신되며 상기 양자 신호 수신부에서 측정된 양자 수신 신호이고, Y_2는 상기 공개 채널을 통해 수신되며 상기 공개 신호 수신부에서 측정된 공개 수신 신호이며,

X_1은 상기 양자 신호 송신부에서 송신하는 양자 송신 신호이고, X_2는 상기 공개 신호 송신부에서 송신하는 공개 송신 신호이며,

상기 Z_1은 양자 채널에서의 노이즈이고, 상기 Z_2는 공개 채널에서의 노이즈이며,

a는 양자 채널과 관련된 채널 특성 상수이고, c는 공개 채널과 관련된 채널 특성 상수이며, b는 간섭 상수이고,

bX_2는 공개 채널을 통해 송신되는 공개 송신 신호(X_2)에 의해 양자 채널에서 발생하는 간섭 성분을 나타내는, 단

일 링크 기반 양자 키 분배 시스템.

청구항 4

청구항 1에 있어서,

상기 공개 채널은, 클록 동기화, 위상 동기화 및 편광 동기화를 위한 동기화 신호를 전송하기 위한 동기 채널 및 보안성을 증폭시키기 위한 추가 정보를 포함하는 관리 신호를 전송하기 위한 관리 채널 중 적어도 하나를 포함하는, 단일 광선로 기반 양자 키 분배 시스템.

청구항 5

청구항 1에 있어서,

상기 단일 링크는 단일 광선로 기반 링크를 포함하는, 단일 링크 기반 양자 키 분배 시스템.

청구항 6

(a) 양자 키 분배 송신부에 포함된 양자 신호 송신부에서 양자 채널을 통해 양자 키와 관련된 양자 신호를 송신하고, 상기 양자 키 분배 송신부에 포함된 공개 신호 송신부에서 공개 채널을 통해 양자 신호를 처리하기 위한 동기화 신호 및 관리 신호를 포함하는 공개 신호를 송신하는 단계; 및

(b) 양자 키 분배 수신부에 포함된 공개 신호 수신부에서, 상기 공개 신호 송신부에서 송신하는 공개 신호를 상기 공개 채널을 통해 수신하고, 상기 양자 키 분배 수신부에 포함된 양자 신호 수신부에서, 상기 양자 신호 송신부에서 송신하는 양자 신호를 상기 양자 채널을 통해 수신하여 상기 양자 키를 검출하는 단계를 포함하며,

상기 양자 채널과 상기 공개 채널은 단일 링크로 형성되는, 단일 링크 기반 양자 키 분배 방법.

청구항 7

청구항 6에 있어서,

상기 양자 키 분배 수신부는,

상기 양자 채널을 통해 수신되는 양자 수신 신호와 상기 공개 채널을 통해 수신되는 공개 수신 신호를 측정하고,

상기 측정된 공개 수신 신호에 기반하여 상기 공개 신호 송신부에서 송신하는 공개 송신 신호를 예측하며,

상기 측정된 양자 수신 신호와 상기 예측된 공개 송신 신호에 기반하여 상기 양자 신호 송신부에서 송신한 양자 송신 신호를 예측하고,

상기 예측된 양자 송신 신호에 기반하여 상기 양자 키를 검출하는, 링크 기반 양자 키 분배 방법.

청구항 8

청구항 7에 있어서,

상기 양자 키 분배 수신부는,

수학식 1에 기반하여 상기 양자 신호 송신부에서 송신한 양자 송신 신호(X_1)를 예측하고,

[수학식 1]

$$Y_1 = aX_1 + bX_2 + Z_1$$

$$Y_2 = cX_2 + Z_2$$

Y_1은 상기 양자 채널을 통해 수신되며 상기 양자 신호 수신부에서 측정된 양자 수신 신호이고, Y_2는 상기 공개 채널을 통해 수신되며 상기 공개 신호 수신부에서 측정된 공개 수신 신호이며,

X_1은 상기 양자 신호 송신부에서 송신하는 양자 송신 신호이고, X_2는 상기 공개 신호 송신부에서 송신하는 공개 송신 신호이며,

상기 Z_1은 양자 채널에서의 노이즈이고, 상기 Z_2는 공개 채널에서의 노이즈이며,

a는 양자 채널과 관련된 채널 특성 상수이고, c는 공개 채널과 관련된 채널 특성 상수이며, b는 간섭 상수이고,

bX_2는 공개 채널을 통해 송신되는 공개 송신 신호(X_2)에 의해 양자 채널에서 발생하는 간섭 성분을 나타내는, 단일 링크 기반 양자 키 분배 방법.

청구항 9

청구항 6에 있어서,

상기 공개 채널은, 클록 동기화, 위상 동기화 및 편광 동기화를 위한 동기화 신호를 전송하기 위한 동기 채널 및 보안성을 증폭시키기 위한 추가 정보를 포함하는 관리 신호를 전송하기 위한 관리 채널 중 적어도 하나를 포함하는, 단일 링크 기반 양자 키 분배 방법.

청구항 10

청구항 6에 있어서,

상기 단일 링크는 단일 광선로 기반 링크를 포함하는, 단일 링크 기반 양자 키 분배 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 단일 링크 기반 양자 키 분배 시스템 및 방법에 관한 것이다.

배 경 기 술

[0002] 도청, 감청 및 해킹 등을 원천 차단할 수 있는 차세대 암호화 기술로서 양자 암호 통신이 주목받고 있다.

[0003] 양자 암호 통신에서 양자 암호 키(이하 양자 키라 함)를 분배하기 위해서는 양자 키와 관련된 양자 신호를 전송하기 위한 양자 채널 및 양자 신호를 후처리하기 위한 공개 신호를 전송하기 위한 공개 채널과 같은 논리 채널들이 필요하다.

[0004] 기존에는 양자 채널을 전용 광선로로 형성하고 공개 신호를 송신하기 위한 공개 채널을 별도의 전송로로 송신하거나 기존 통신 채널과 파장다중화하여 송신하였다. 하지만, 이렇게 양자 채널과 공개 채널을 별개로 형성하는 경우, 양자 채널 및 공개 채널을 위해 별도의 전용 링크를 구축해야 하므로, 망 구축 비용 및 유지 보수 비용이 증가하는 문제점이 있었다.

[0005] 따라서 양자 키 분배를 위하여 별도의 전용 광 네트워크를 구축할 필요 없이 기존에 구축되어 있는 상용 통신망의 활용이 가능하여 망 구축 비용 및 유지 보수 비용을 절감할 수 있는 양자 키 분배 시스템이 요구되고 있다.

선행기술문헌

특허문헌

[0006] (특허문헌 0001) KR 10-1031978 B1

발명의 내용

해결하려는 과제

[0007] 본 발명이 해결하고자 하는 과제는 기존에 구축되어 있는 상용 통신망의 활용이 가능하여 망 구축 비용 및 유지 보수 비용을 절감할 수 있는, 단일 링크 기반 양자 키 분배 시스템을 제공하는 것이다.

[0008] 본 발명이 해결하고자 하는 과제는 기존에 구축되어 있는 상용 통신망의 활용이 가능하여 망 구축 비용 및 유지 보수 비용을 절감할 수 있는, 단일 링크 기반 양자 키 분배 방법을 제공하는 것이다.

과제의 해결 수단

[0009] 상기 과제를 해결하기 위한 본 발명의 일 실시예에 의한 단일 링크 기반 양자 키 분배 시스템은,

[0010] 양자 채널을 통해 양자 키와 관련된 양자 신호를 송신하기 위한 양자 신호 송신부 및 공개 채널을 통해 양자 신호를 처리하기 위한 동기화 신호 및 관리 신호를 포함하는 공개 신호를 송신하기 위한 공개 신호 송신부를 포함하는 양자 키 분배 송신부; 및

[0011] 상기 양자 신호 송신부에서 송신하는 양자 신호를 상기 양자 채널을 통해 수신하여 상기 양자 키를 검출하기 위한 양자 신호 수신부 및 상기 공개 신호 송신부에서 송신하는 공개 신호를 상기 공개 채널을 통해 수신하기 위한 공개 신호 수신부를 포함하는 양자 키 분배 수신부를 포함하고,

[0012] 상기 양자 채널과 상기 공개 채널은 단일 링크로 형성된다.

[0013] 본 발명의 일 실시예에 의한 단일 링크 기반 양자 키 분배 시스템에 있어서, 상기 양자 키 분배 수신부는,

[0014] 상기 양자 채널을 통해 수신되는 양자 수신 신호와 상기 공개 채널을 통해 수신되는 공개 수신 신호를 측정하고,

[0015] 상기 측정된 공개 수신 신호에 기반하여 상기 공개 신호 송신부에서 송신하는 공개 송신 신호를 예측하며,

[0016] 상기 측정된 양자 수신 신호와 상기 예측된 공개 송신 신호에 기반하여 상기 양자 신호 송신부에서 송신한 양자 송신 신호를 예측하고,

[0017] 상기 예측된 양자 송신 신호에 기반하여 상기 양자 키를 검출할 수 있다.

[0018] 또한, 본 발명의 일 실시예에 의한 단일 링크 기반 양자 키 분배 시스템에 있어서, 상기 양자 키 분배 수신부는,

[0019] 수학식 1에 기반하여 상기 양자 신호 송신부에서 송신한 양자 송신 신호(X_1)를 예측하고,

[0020] [수학식 1]

[0021]
$$Y_1 = aX_1 + bX_2 + Z_1$$
$$Y_2 = cX_2 + Z_2$$

[0022] Y_1은 상기 양자 채널을 통해 수신되며 상기 양자 신호 수신부에서 측정된 양자 수신 신호이고, Y_2는 상기 공개 채널을 통해 수신되며 상기 공개 신호 수신부에서 측정된 공개 수신 신호이며,

[0023] X_1은 상기 양자 신호 송신부에서 송신하는 양자 송신 신호이고, X_2는 상기 공개 신호 송신부에서 송신하는 공개 송신 신호이며,

[0024] 상기 Z_1은 양자 채널에서의 노이즈이고, 상기 Z_2는 공개 채널에서의 노이즈이며,

[0025] a는 양자 채널과 관련된 채널 특성 상수이고, c는 공개 채널과 관련된 채널 특성 상수이며, b는 간섭 상수이고,

[0026] bX_2는 공개 채널을 통해 송신되는 공개 송신 신호(X_2)에 의해 양자 채널에서 발생하는 간섭 성분을 나타낼 수 있다.

[0027] 또한, 본 발명의 일 실시예에 의한 단일 링크 기반 양자 키 분배 시스템에 있어서, 상기 공개 채널은, 클록 동기화, 위상 동기화 및 편광 동기화를 위한 동기화 신호를 전송하기 위한 동기 채널 및 보안성을 증폭시키기 위

한 추가 정보를 포함하는 관리 신호를 전송하기 위한 관리 채널 중 적어도 하나를 포함할 수 있다.

[0028] 또한, 본 발명의 일 실시예에 의한 단일 링크 기반 양자 키 분배 시스템에 있어서, 상기 단일 링크는 단일 광선로 기반 링크를 포함할 수 있다.

[0029] 상기 다른 과제를 해결하기 위한 본 발명의 일 실시예에 의한 단일 링크 기반 양자 키 분배 방법은,

[0030] (a) 양자 키 분배 송신부에 포함된 양자 신호 송신부에서 양자 채널을 통해 양자 키와 관련된 양자 신호를 송신하고, 상기 양자 키 분배 송신부에 포함된 공개 신호 송신부에서 공개 채널을 통해 양자 신호를 처리하기 위한 동기화 신호 및 관리 신호를 포함하는 공개 신호를 송신하는 단계; 및

[0031] (b) 양자 키 분배 수신부에 포함된 공개 신호 수신부에서, 상기 공개 신호 송신부에서 송신하는 공개 신호를 상기 공개 채널을 통해 수신하고, 상기 양자 키 분배 수신부에 포함된 양자 신호 수신부에서, 상기 양자 신호 송신부에서 송신하는 양자 신호를 상기 양자 채널을 통해 수신하여 상기 양자 키를 검출하는 단계를 포함하며,

[0032] 상기 양자 채널과 상기 공개 채널은 단일 링크로 형성된다.

[0033] 본 발명의 일 실시예에 의한 단일 링크 기반 양자 키 분배 방법에 있어서, 상기 양자 키 분배 수신부는,

[0034] 상기 양자 채널을 통해 수신되는 양자 수신 신호와 상기 공개 채널을 통해 수신되는 공개 수신 신호를 측정하고,

[0035] 상기 측정된 공개 수신 신호에 기반하여 상기 공개 신호 송신부에서 송신하는 공개 송신 신호를 예측하며,

[0036] 상기 측정된 양자 수신 신호와 상기 예측된 공개 송신 신호에 기반하여 상기 양자 신호 송신부에서 송신한 양자 송신 신호를 예측하고,

[0037] 상기 예측된 양자 송신 신호에 기반하여 상기 양자 키를 검출할 수 있다.

[0038] 또한, 본 발명의 일 실시예에 의한 단일 링크 기반 양자 키 분배 방법에 있어서, 상기 양자 키 분배 수신부는,

[0039] 수학식 1에 기반하여 상기 양자 신호 송신부에서 송신한 양자 송신 신호(X_1)를 예측하고,

[0040] [수학식 1]

[0041]
$$Y_1 = aX_1 + bX_2 + Z_1$$

$$Y_2 = cX_2 + Z_2$$

[0042] Y_1은 상기 양자 채널을 통해 수신되며 상기 양자 신호 수신부에서 측정된 양자 수신 신호이고, Y_2는 상기 공개 채널을 통해 수신되며 상기 공개 신호 수신부에서 측정된 공개 수신 신호이며,

[0043] X_1은 상기 양자 신호 송신부에서 송신하는 양자 송신 신호이고, X_2는 상기 공개 신호 송신부에서 송신하는 공개 송신 신호이며,

[0044] 상기 Z_1은 양자 채널에서의 노이즈이고, 상기 Z_2는 공개 채널에서의 노이즈이며,

[0045] a는 양자 채널과 관련된 채널 특성 상수이고, c는 공개 채널과 관련된 채널 특성 상수이며, b는 간섭 상수이고,

[0046] bX_2는 공개 채널을 통해 송신되는 공개 송신 신호(X_2)에 의해 양자 채널에서 발생하는 간섭 성분을 나타낼 수 있다.

[0047] 또한, 본 발명의 일 실시예에 의한 단일 링크 기반 양자 키 분배 방법에 있어서, 상기 공개 채널은, 클록 동기화, 위상 동기화 및 편광 동기화를 위한 동기화 신호를 전송하기 위한 동기 채널 및 보안성을 증폭시키기 위한 추가 정보를 포함하는 관리 신호를 전송하기 위한 관리 채널 중 적어도 하나를 포함할 수 있다.

[0048] 또한, 본 발명의 일 실시예에 의한 단일 링크 기반 양자 키 분배 방법에 있어서, 상기 단일 링크는 단일 광선로 기반 링크를 포함할 수 있다.

발명의 효과

[0049] 본 발명의 일 실시예에 의한 단일 링크 기반 양자 키 분배 시스템 및 방법에 의하면, 다양한 구성과 형태의 상용 통신망을 활용한 양자 키 분배 시스템을 가능하게 하여 망 구축 비용 및 유지 보수 비용을 절감하고 시장의 규모를 확대하여 운영자의 이윤을 보장하면서 많은 사용자들에게 암호 키를 제공할 수 있다.

도면의 간단한 설명

[0050] 도 1은 본 발명의 일 실시예에 의한 단일 링크 기반 양자 키 분배 시스템이 적용되는 양자 암호 통신의 개념도.

도 2는 본 발명의 일 실시예에 의한 단일 링크 기반 양자 키 분배 시스템을 도시한 도면.

도 3은 본 발명의 일 실시예에 의한 단일 링크 기반 양자 키 분배 방법을 설명하기 위한 도면.

도 4a 및 도 4b는 본 발명의 일 실시예에 의한 단일 링크 기반 양자 키 분배 방법의 기술적 근거를 설명하기 위한 도면.

발명을 실시하기 위한 구체적인 내용

[0051] 본 발명의 목적, 특정한 장점들 및 신규한 특징들은 첨부된 도면들과 연관되어지는 이하의 상세한 설명과 바람직한 실시예들로부터 더욱 명백해질 것이다.

[0052] 이에 앞서 본 명세서 및 청구범위에 사용된 용어나 단어는 통상적이고 사전적인 의미로 해석되어서는 아니되며, 발명자가 그 자신의 발명을 가장 최선의 방법으로 설명하기 위해 용어의 개념을 적절하게 정의할 수 있는 원칙에 입각하여 본 발명의 기술적 사상에 부합되는 의미와 개념으로 해석되어야 한다.

[0053] 본 명세서에서 각 도면의 구성요소들에 참조번호를 부가함에 있어서, 동일한 구성 요소들에 한해서는 비록 다른 도면상에 표시되더라도 가능한 한 동일한 번호를 가지도록 하고 있음에 유의하여야 한다.

[0054] 또한, "제1", "제2", "일면", "타면" 등의 용어는, 하나의 구성요소를 다른 구성요소로부터 구별하기 위해 사용되는 것으로, 구성요소가 상기 용어들에 의해 제한되는 것은 아니다.

[0055] 이하, 본 발명을 설명함에 있어, 본 발명의 요지를 불필요하게 흐릴 수 있는 관련된 공지 기술에 대한 상세한 설명은 생략한다.

[0056] 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시형태를 상세히 설명하기로 한다.

[0057] 도 1에 도시된 본 발명의 일 실시예에 의한 단일 링크 기반 양자 키 분배 시스템이 적용되는 양자 암호 통신의 개념도를 참조하면, 양자 암호 통신에 있어서, 양자 키 분배 송신부(100)의 양자 신호 송신부(104)는 양자 암호 키(이하 양자 키라 함)를 생성하여 생성한 양자 키를 양자 신호로서 양자 채널(112)을 통해 송신하며, 암복호화부(116)는 양자 키 분배 송신부(100)로부터 수신한 양자 암호 키에 기반하여 데이터를 암호화하여 암호화된 데이터를 데이터 채널(120)을 통해 송신한다.

[0058] 또한, 양자 키 분배 송신부(100)의 공개 신호 송신부(106)는 공개 채널(114)을 통해 양자 신호를 후처리하기 위한 공개 신호를 전송한다. 공개 채널(114)은 동기 채널 및 관리 채널을 포함하며, 동기 채널을 통해 전송되는 동기화 신호는 클록의 동기화, 위상 동기화 및 편광 동기화를 위해 사용된다. 그리고 보안성을 증폭시키기 위한 추가 정보들을 포함하는 관리 신호는 관리 채널을 통해 전송된다.

[0059] 양자 키 분배 수신부(102)의 양자 신호 수신부(108)는 양자 채널(112)을 통해 양자 신호를 수신하고, 공개 신호 수신부(110)는 공개 채널(114)을 동기화 신호 및 관리 신호를 포함하는 공개 신호를 수신하며, 양자 채널(112)을 통해 수신한 양자 신호에 기반하여 상기 양자 암호 키를 검출하여 검출된 양자 암호 키를 암복호화부(118)에 분배하고, 암복화부(118)는 양자 신호 수신부(108)로부터 수신된 양자 암호 키에 기반하여 데이터 채널(120)을 통해 수신된 데이터를 복호화한다.

[0060] 도 2는 본 발명의 일 실시예에 의한 단일 링크 기반 양자 키 분배 시스템을 도시한 도면이다.

[0061] 도 2에 도시된 본 발명의 일 실시예에 의한 단일 링크 기반 양자 키 분배 시스템은, 양자 키 분배 송신부(200) 및 양자 키 분배 수신부(202)를 포함한다.

[0062] 상기 양자 키 분배 송신부(200)는, 양자 채널(212)을 통해 양자 키와 관련된 양자 신호를 송신하기 위한 양자

신호 송신부(204) 및 공개 채널(214)을 통해 양자 신호를 처리하기 위한 동기화 신호 및 관리 신호를 포함하는 공개 신호를 송신하기 위한 공개 신호 송신부(206)를 포함한다.

[0063] 상기 양자 키 분배 수신부(202)는, 상기 양자 신호 송신부(204)에서 송신하는 양자 신호를 상기 양자 채널(212)을 통해 수신하여 상기 양자 키를 검출하기 위한 양자 신호 수신부(208) 및 상기 공개 신호 송신부(210)에서 송신하는 공개 신호를 상기 공개 채널(214)을 통해 수신하기 위한 공개 신호 수신부(210)를 포함한다.

[0064] 한편, 상기 양자 채널(212)과 상기 공개 채널(214)은 단일 링크, 예를 들어, 단일 광선로로 형성된다.

[0065] 상기 공개 채널(214)은, 클록 동기화, 위상 동기화 및 편광 동기화를 위한 동기화 신호를 전송하기 위한 동기 채널 및 보안성을 증폭시키기 위한 추가 정보를 포함하는 관리 신호를 전송하기 위한 관리 채널 중 적어도 하나를 포함한다.

[0066] 상기와 같이 구성된 본 발명의 일 실시예에 의한 단일 링크 기반 양자 키 분배 시스템의 동작을 도 2 내지 도 4를 참조하여 하기에 설명하기로 한다.

[0067] 우선, 양자 키 분배 송신부(200)에 포함된 양자 신호 송신부(204)에서 양자 채널(212)을 통해 양자 키와 관련된 양자 신호를 송신하고, 상기 양자 키 분배 송신부(200)에 포함된 공개 신호 송신부(206)에서 공개 채널(214)을 통해 양자 신호를 처리하기 위한 동기화 신호 및 관리 신호를 포함하는 공개 신호를 송신한다.

[0068] 양자 키 분배 수신부(202)에 포함된 공개 신호 수신부(210)에서, 상기 공개 신호 송신부(206)에서 송신하는 공개 신호를 상기 공개 채널(214)을 통해 수신하고, 상기 양자 키 분배 수신부(202)에 포함된 양자 신호 수신부(208)에서, 상기 양자 신호 송신부(204)에서 송신하는 양자 신호를 상기 양자 채널(212)을 통해 수신하여, 상기 양자 키를 검출한다.

[0069] 상기 양자 키 분배 수신부(202)에서 양자 키를 검출하는 동작을 도 2 및 도 3을 참조하여 설명하기로 한다.

[0070] 상기 양자 키 분배 수신부(202)는, 상기 양자 채널(212)을 통해 수신되는 양자 수신 신호(Y_1)와 상기 공개 채널(214)을 통해 수신되는 공개 수신 신호(Y_2)를 측정하고, 상기 측정된 공개 수신 신호에 기반하여 상기 양자 키 분배 송신부(200)에 포함된 상기 공개 신호 송신부(206)에서 송신하는 공개 송신 신호(X_2)를 예측하며, 상기 측정된 양자 수신 신호(Y_1)와 상기 예측된 공개 송신 신호에 기반하여 상기 양자 키 분배 송신부(200)에 포함된 상기 양자 신호 송신부(204)에서 송신한 양자 송신 신호(X_1)를 예측한다.

[0071] 최종적으로 상기 양자 키 분배 수신부(202)에 포함된 양자 신호 수신부(208)는 예측된 양자 송신 신호에 기반하여 상기 양자 키를 검출한다.

[0072] 상기 양자 키 분배 수신부(202)에서 양자 키를 검출하는 과정을 하기에 구체적으로 설명하기로 한다.

[0073] 도 3에 도시된 바와 같이, 양자 채널(212)을 통해 송신되는 양자 신호는 그 크기가 매우 미약하기 때문에, 양자 채널(212)을 통해 송신되는 양자 신호에 의해 공개 채널(214)에서 발생하는 간섭은 무시할 수 있다.

[0074] 하지만, 공개 채널(214)을 통해 송신되는 공개 신호는 그 크기가 양자 채널(212)에 영향을 줄 수 있을 정도이기 때문에, 공개 채널(214)을 통해 송신되는 공개 신호에 의해 양자 채널(212)에 간섭이 발생하여 양자 채널(212)을 통해 송신되는 양자 신호가 간섭에 의해 영향을 받을 수 있다.

[0075] 따라서 도 3에 도시된 바와 같이 양자 채널(212)과 공개 채널(214)은 한 방향으로만, 즉, 공개 채널(214)에서 양자 채널(212)로의 방향으로만 간섭이 크게 발생한다.

[0076] 상기한 점을 고려하여 상기 양자 키 분배 수신부(202)는 수학식 1에 기반하여 양자 키를 검출한다.

수학식 1

[0077]
$$Y_1 = aX_1 + bX_2 + Z_1$$
$$Y_2 = cX_2 + Z_2$$

[0078] 상기 양자 키 분배 수신부(202)에서는 수학식 1에 기반하여 상기 양자 신호 송신부(200)에서 송신하는 양자 송신 신호(X_1)를 예측하고, 예측된 양자 송신 신호에 기반하여 양자 키를 검출한다.

[0079] Y_1은 상기 양자 채널(212)을 통해 수신되며 상기 양자 신호 수신부(208)에서 측정된 양자 수신 신호이고, Y_2는 상기 공개 채널(214)을 통해 수신되며 상기 공개 신호 수신부(210)에서 측정된 공개 수신 신호이다.

[0080] X_1은 상기 양자 신호 송신부(204)에서 송신하는 양자 송신 신호이고, X_2는 상기 공개 신호 송신부(206)에서 송신하는 공개 송신 신호이며, 상기 Z_1은 양자 채널(212)에서의 노이즈이고, 상기 Z_2는 공개 채널(214)에서의 노이즈이다.

[0081] a는 양자 채널(212)과 관련된 채널 특성 상수이고, c는 공개 채널(214)과 관련된 채널 특성 상수이며, b는 간섭 상수이고, bX_2는 공개 채널(214)을 통해 송신되는 공개 송신 신호(X_2)에 의해 양자 채널(212)에서 발생하는 간섭 성분을 나타낸다.

[0082] 일반적으로 공개 채널(214)을 통해 전송되는 공개 신호는 양자 채널(212)을 통해 전송되는 양자 신호보다 높은 정확도로 검출 가능하기 때문에, 양자 키 분배 수신부(202)의 공개 신호 수신부(210)에서 측정된 공개 수신 신호(Y_2)로부터 공개 송신 신호(X_2)를 예측하고, 예측된 공개 송신 신호를 활용하면, 상기 양자 신호 송신부(204)에서 송신한 양자 송신 신호(X_1)의 분포를 보다 정확하게 예측할 수 있기 때문에, 오류율을 낮출 수 있다.

[0083] 도 4a에 도시된 바와 같이, 간섭을 무시하고 상기 양자 채널(212)을 통해 수신되며 상기 양자 신호 수신부(208)에서 측정된 양자 수신 신호(Y_1)만을 고려하여 상기 양자 신호 송신부(204)에서 송신한 양자 송신 신호(X_1)를 예측하는 경우, 확률 분포가 넓게 퍼지게 되어, 오류율이 증가하여 정확한 값을 예측하기가 쉽지 않다.

[0084] 하지만, 도 4b에 도시된 바와 같이, 공개 채널(214)을 통해 송신되는 신호(X_2)에 의해 양자 채널(212)에서 발생하는 간섭을 고려하는 경우, 확률 분포가 좁아지게 되어, 오류율을 낮출 수 있어, 정확한 값을 예측할 수 있다.

[0085] 이상 본 발명을 구체적인 실시예를 통하여 상세하게 설명하였으나, 이는 본 발명을 구체적으로 설명하기 위한 것으로, 본 발명은 이에 한정되지 않으며, 본 발명의 기술적 사상 내에서 당 분야의 통상의 지식을 가진 자에 의해 그 변형이나 개량이 가능함은 명백하다고 할 것이다.

[0086] 본 발명의 단순한 변형 내지 변경은 모두 본 발명의 영역에 속하는 것으로, 본 발명의 구체적인 보호 범위는 첨부된 청구범위에 의하여 명확해질 것이다.

부호의 설명

[0087] 100, 200 : 양자 키 분배 송신부 102, 202 : 양자 키 분배 수신부

104, 204 : 양자 신호 송신부 106, 206 : 공개 신호 송신부

108, 208 : 양자 신호 수신부 110, 210 : 공개 신호 수신부

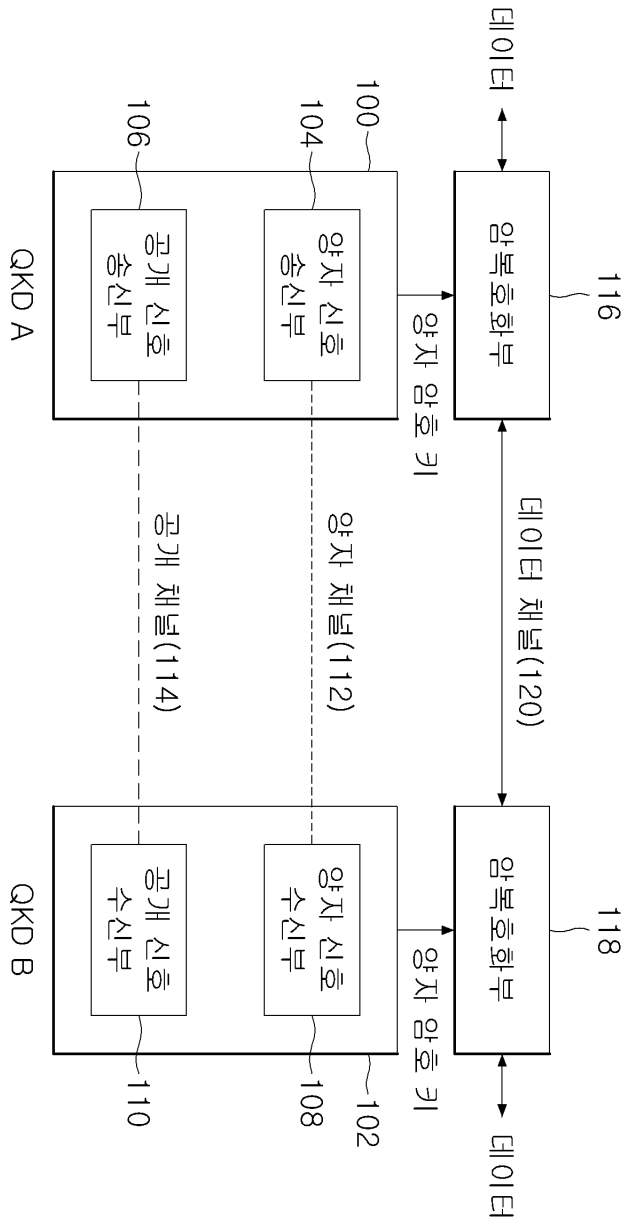
112, 212 : 양자 채널 114, 214 : 공개 채널

116, 118 : 암복호화부 120 : 데이터 채널

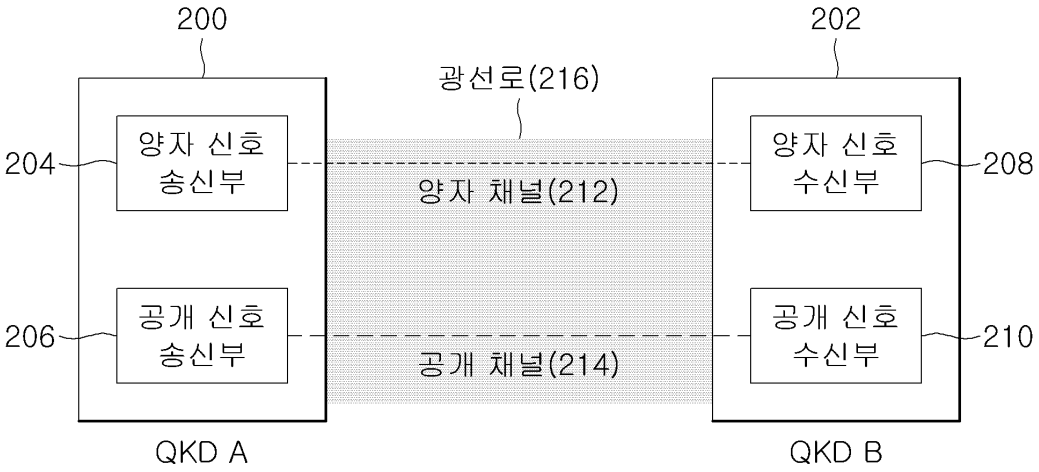
216 : 광선로

도면

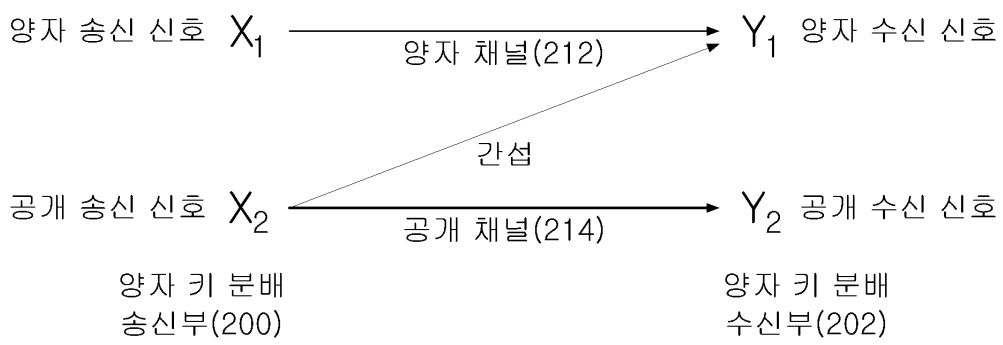
도면1


데이터
100
104
106
116
암복호화부
양자 신호 송신부
공개 신호 송신부
QKD A
양자 암호 키
데이터 채널(120)
양자 채널(112)
공개 채널(114)
양자 암호 키
118
암복호화부
양자 신호 수신부
공개 신호 수신부
QKD B
102
108
110
데이터

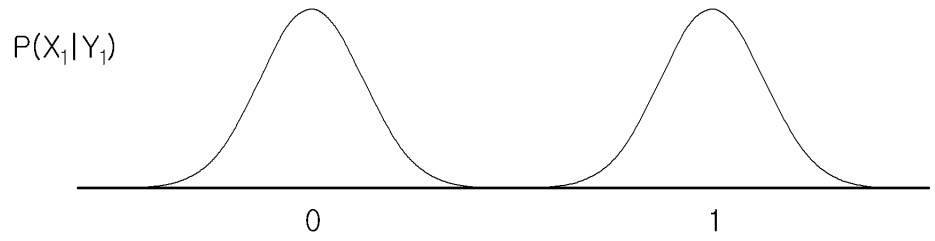
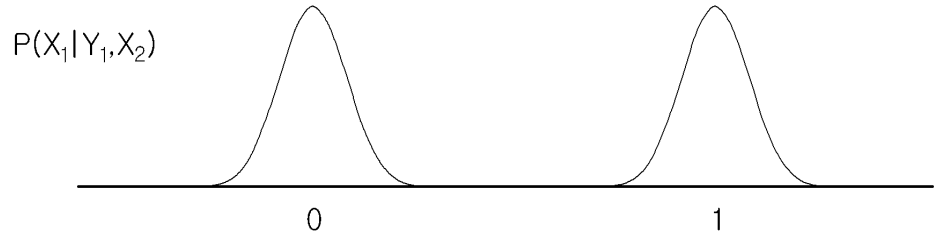
도면2



도면3



도면4a



도면4b