



(19) 대한민국특허청(KR)  
(12) 공개특허공보(A)

(11) 공개번호 10-2024-0013069  
(43) 공개일자 2024년01월30일

(51) 국제특허분류(Int. Cl.)  
H04L 9/08 (2006.01) H04L 1/00 (2006.01)  
(52) CPC특허분류  
H04L 9/0852 (2023.08)  
H04L 1/004 (2013.01)  
(21) 출원번호 10-2023-0094440  
(22) 출원일자 2023년07월20일  
심사청구일자 2023년07월20일  
(30) 우선권주장  
1020220090248 2022년07월21일 대한민국(KR)

(71) 출원인  
주식회사 큐심플러스  
서울특별시 중구 을지로 50, 17층 1722호(을지로  
2가, 을지한국빌딩)  
(72) 발명자  
노광석  
서울특별시 도봉구 해동로 241-14 금호타운2차아  
파트 203동102호  
신유철  
경기도 하남시 위례대로6길 70 (학암동, 위례중흥  
에스-클래스)7805동 503호  
허준  
서울특별시 강남구 광평로10길 6 한솔마을아파트  
206동 103호  
(74) 대리인  
특허법인위솔

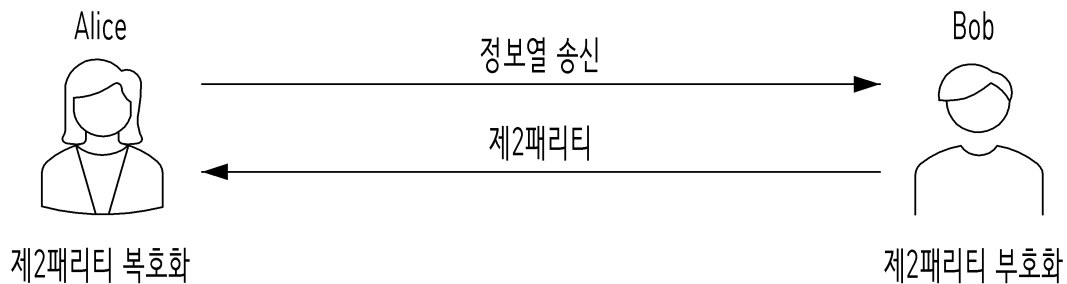
전체 청구항 수 : 총 6 항

(54) 발명의 명칭 양자 암호 통신에서의 오류 정정을 위한 방법 및 시스템

(57) 요약

제1통신 장치와 제2통신 장치 사이의 양자 암호 통신 방법은, 상기 제1통신 장치가 광자의 위상이나 편광을 랜덤하게 변조함으로써 생성된 제1정보열을 상기 제2통신 장치에 전송하면 상기 제2통신 장치가 상기 제1정보열에 기반하여 제2정보열을 생성하는 양자 통신 단계, 및 소정의 기준에 기반하여 선택된 오류 정정 모드에 기반하여 상기 제1정보열과 제2정보열을 동일하도록 맞추는 후처리 단계를 포함할 수 있다. 상기 오류 정정 모드는 패리티 정보의 복호화 주체에 따라 구분될 수 있다.

대표도 - 도5



이 발명을 지원한 국가연구개발사업

|             |                              |
|-------------|------------------------------|
| 과제고유번호      | 1711193089                   |
| 과제번호        | 2021-0-01810-003             |
| 부처명         | 과학기술정보통신부                    |
| 과제관리(전문)기관명 | 정보통신기획평가원                    |
| 연구사업명       | 대학ICT연구센터육성지원사업              |
| 연구과제명       | 양자세계를 연결하는 초신뢰 양자인터넷 요소 기술개발 |
| 기 여 율       | 1/1                          |
| 과제수행기관명     | 고려대학교산학협력단                   |
| 연구기간        | 2023.01.01 ~ 2023.12.31      |

---

## 명세서

### 청구범위

#### 청구항 1

적어도 하나의 프로세서에 의해 수행되는 적어도 하나의 제1통신 장치와 적어도 하나의 제2통신 장치 사이의 양자 암호 통신 방법에 있어서,

상기 제1통신 장치가 광자의 위상이나 편광에 의해 랜덤하게 변조함으로써 생성된 제1정보열을 상기 제2통신 장치에 전송하면 상기 제2통신 장치가 상기 제1정보열에 기반하여 제2정보열을 생성하는 양자 통신 단계;

소정의 기준에 기반하여 선택된 오류 정정 모드 하에서 패리티 정보를 이용하여 상기 제1정보열과 제2정보열을 동일하도록 맞추는 후처리 단계를 포함하고,

상기 오류 정정 모드는, 상기 제1통신 장치가 제1패리티 정보를 부호화하여 상기 제2통신 장치에게 전송하면 상기 제2통신 장치가 상기 부호화된 제1패리티 정보를 복호화함으로써 상기 제2정보열을 상기 제1정보열과 동일하게 맞추는 제1오류 정정 모드와 상기 제2통신 장치가 제2패리티 정보를 부호화하여 상기 제1통신 장치에게 전송하면 상기 제1통신 장치가 상기 부호화된 제2패리티 정보를 복호화함으로써 상기 제1정보열을 상기 제2정보열과 동일하게 맞추는 제2오류 정정 모드 중 하나이고,

상기 소정의 기준은 상기 제1통신 장치와 상기 제2통신 장치 중 디텍터가 위치하지 않은 통신 장치가 상기 패리티 정보의 부호화를 수행하고, 상기 제1통신 장치와 상기 제2통신 장치 중 디텍터가 위치한 통신 장치가 상기 패리티 정보의 복호화를 수행하는 제1기준과 상기 패리티 정보에 대한 복호화 주체에 대한 정보가 포함된 시그널링 정보에 기반하여 상기 제1통신 장치와 상기 제2통신 장치 중 어느 하나가 상기 패리티 정보의 복호화를 수행하는 제2기준을 포함하는 양자 암호 통신 방법.

#### 청구항 2

제1항에 있어서,

적어도 하나의 제2통신 장치는 복수의 통신 장치들을 포함하고,

상기 제1통신 장치와 상기 복수의 통신 장치들 사이의 상기 후처리 단계는 상기 제1기준에 따라 수행되는 양자 암호 통신 방법.

#### 청구항 3

제1항에 있어서,

적어도 하나의 제2통신 장치는 복수의 통신 장치들을 포함하고,

상기 제1통신 장치와 상기 복수의 통신 장치들 사이의 상기 후처리 단계는 상기 제2기준에 따라 수행되는 양자 암호 통신 방법.

#### 청구항 4

적어도 하나의 프로세서에 의해 수행되는 적어도 하나의 제1통신 장치와 적어도 하나의 제2통신 장치 사이의 양자 암호 통신 방법에 있어서,

상기 제1통신 장치가 광자의 위상이나 편광에 의해 랜덤하게 변조함으로써 생성된 제1정보열을 상기 제2통신 장치에 전송하면 상기 제2통신 장치가 상기 제1정보열에 기반하여 제2정보열을 생성하는 양자 통신 단계;

소정의 기준에 기반하여 선택된 오류 정정 모드 하에서 패리티 정보를 이용하여 상기 제1정보열과 제2정보열을 동일하도록 맞추는 후처리 단계를 포함하고,

상기 오류 정정 모드는, 상기 제1통신 장치가 제1패리티 정보를 부호화하여 상기 제2통신 장치에게 전송하면 상기 제2통신 장치가 상기 부호화된 제1패리티 정보를 복호화함으로써 상기 제2정보열을 상기 제1정보열과 동일하게 맞추는 제1오류 정정 모드와 상기 제2통신 장치가 제2패리티 정보를 부호화하여 상기 제1통신 장치에게 전송

하면 상기 제1통신 장치가 상기 부호화된 제2패리티 정보를 복호화함으로써 상기 제1정보열을 상기 제2정보열과 동일하게 맞추는 제2오류 정정 모드 중 하나이고,

상기 소정의 기준은 도청자가 상기 제1통신 장치보다 상기 제2통신 장치에 더 가까이 위치하고 있으면 상기 오류 정정 모드는 상기 제1오류 정정 모드로 선택되고, 도청자가 상기 제2통신 장치보다 상기 제1통신 장치에 더 가까이 있으면 상기 오류 정정 모드는 상기 제2오류 정정 모드로 선택되는 양자 암호 통신 방법.

## 청구항 5

광자의 위상이나 편광에 의해 랜덤하게 변조함으로써 생성된 제1정보열을 제2통신 장치에 전송하기 위한 제1통신 장치; 및

상기 수신된 제1정보열에 기반하여 제2정보열을 생성하기 위한 제2통신 장치를 포함하고,

소정의 기준에 기반하여 선택된 오류 정정 모드 하에서 패리티 정보를 이용하여 상기 제1정보열과 제2정보열을 동일하도록 맞추는 오류 정정 과정을 통해 양자키 분배가 수행되되,

상기 오류 정정 모드는, 상기 제1통신 장치가 제1패리티 정보를 부호화하여 상기 제2통신 장치에게 전송하면 상기 제2통신 장치가 상기 부호화된 제1패리티 정보를 복호화함으로써 상기 제2정보열을 상기 제1정보열과 동일하게 맞추는 제1오류 정정 모드와 상기 제2통신 장치가 제2패리티 정보를 부호화하여 상기 제1통신 장치에게 전송하면 상기 제1통신 장치가 상기 부호화된 제2패리티 정보를 복호화함으로써 상기 제1정보열을 상기 제2정보열과 동일하게 맞추는 제2오류 정정 모드 중 하나이고,

상기 소정의 기준은 상기 제1통신 장치와 상기 제2통신 장치 중 디텍터가 위치하지 않은 통신 장치가 상기 패리티 정보의 부호화를 수행하고, 상기 제1통신 장치와 상기 제2통신 장치 중 디텍터가 위치한 통신 장치가 상기 패리티 정보의 복호화를 수행하는 제1기준과 상기 패리티 정보에 대한 복호화 주체에 대한 정보가 포함된 시그널링 정보에 기반하여 상기 제1통신 장치와 상기 제2통신 장치 중 어느 하나가 상기 패리티 정보의 복호화를 수행하는 제2기준을 포함하는 양자 암호 통신 시스템.

## 청구항 6

광자의 위상이나 편광에 의해 랜덤하게 변조함으로써 생성된 제1정보열을 제2통신 장치에 전송하기 위한 제1통신 장치; 및

상기 수신된 제1정보열에 기반하여 제2정보열을 생성하기 위한 제2통신 장치를 포함하고,

소정의 기준에 기반하여 선택된 오류 정정 모드 하에서 패리티 정보를 이용하여 상기 제1정보열과 제2정보열을 동일하도록 맞추는 오류 정정 과정을 통해 양자키 분배가 수행되되,

상기 오류 정정 모드는, 상기 제1통신 장치가 제1패리티 정보를 부호화하여 상기 제2통신 장치에게 전송하면 상기 제2통신 장치가 상기 부호화된 제1패리티 정보를 복호화함으로써 상기 제2정보열을 상기 제1정보열과 동일하게 맞추는 제1오류 정정 모드와 상기 제2통신 장치가 제2패리티 정보를 부호화하여 상기 제1통신 장치에게 전송하면 상기 제1통신 장치가 상기 부호화된 제2패리티 정보를 복호화함으로써 상기 제1정보열을 상기 제2정보열과 동일하게 맞추는 제2오류 정정 모드 중 하나이고,

상기 소정의 기준은 도청자가 상기 제1통신 장치보다 상기 제2통신 장치에 더 가까이 위치하고 있으면 상기 오류 정정 모드는 상기 제1오류 정정 모드로 선택되고, 도청자가 상기 제2통신 장치보다 상기 제1통신 장치에 더 가까이 있으면 상기 오류 정정 모드는 상기 제2오류 정정 모드로 선택되는 양자 암호 통신 시스템.

## 발명의 설명

## 기술 분야

[0001] 본 발명은 양자 암호 통신 방법 및 시스템에 관한 것이다.

## 배경 기술

[0002] 양자 암호 통신(quantum cryptography communication)은 빛 알갱이를 이용하여 더 이상 쪼갤 수 없는 양자(Quantum)를 생성해 송신자와 수신자 사이에 해독이 가능한 암호 키를 만들어 분배함으로써 해킹을 막는 기술이다. 양자 암호 통신은 양자 통신을 통해 송신자와 수신자 사이에 암호 키를 안전하게 서로 분배하여 가질 수 있

는 기술로서, 양자 키 분배(Quantum Key Distribution, QKD)라고도 한다.

[0003] 양자 암호 통신은 송신자와 수신자가 각자의 정보열을 생성하는 양자 통신 단계와 각자의 정보열을 서로 동일하게 맞추기 위한 후처리 단계로 구성된다. 양자 암호 통신 과정을 도1과 2를 동시에 참조하여 설명하면 다음과 같다.

[0004] 먼저 양자 통신 단계(S10)에서, 송신자 Alice가 랜덤하게 정보열을 생성할 수 있다. 광을 이용하는 경우 위상, 편광 등에 의해 랜덤하게 변조된 정보를 인코딩하여 제1정보열을 생성할 수 있다. 송신자 Alice는 제1정보열을 수신자 Bob에게 유선 내지 무선 등의 통신 채널을 통하여 전송할 수 있다. 수신자 Bob은 수신한 제1정보열을 기반으로 자신만의 제2정보열을 생성한다. 예로서, 수신자 Bob은 제1정보열에 대해 측정을 수행(편광 기저를 랜덤하게 선택함으로써)하여 제2정보열을 생성할 수 있다. 즉, 수신자 Bob은 송신자 Alice와는 다른 정보열을 갖게 된다.

[0005] 다음으로, 후처리 단계(S20)는 송신자와 수신자가 갖고 있는 서로 다른 정보열을 동일하게 맞추는 과정이다. 후처리 단계는 시프팅(Sifting) 과정, 오류 정정(Information Reconciliation) 과정, 비밀 증폭(privacy amplification) 과정을 포함할 수 있다. 시프팅 과정은 송신자 Alice와 수신자 Bob의 각 정보열(제1정보열과 제2정보열) 생성시 사용한 기저(basis)를 이용하여 동일한 기저를 갖는 정보열만 남기는 과정이다. 오류 정정 과정은 오류 정정 부호를 이용하여 송신자 Alice와 수신자 Bob의 시프팅 과정 후 남아있는 정보열을 동일하게 하는 과정이다. 비밀 증폭 과정은 양자 통신 단계 또는 후처리 단계에서 도청자 Eve에게 노출되었거나 노출되었을 것이라고 판단되는 만큼의 정보량을 오류 정정 과정이 수행된 후 남아있는 송신자 Alice와 수신자 Bob의 각각의 정보열에서 제거하는 과정이다. 비밀 증폭 과정 후 남아있는 각자의 정보열이 Alice와 Bob에게 최종적으로 분배된 암호 키이다.

## 발명의 내용

### 해결하려는 과제

[0006] 오류 정정 과정에서 필요한 부호화 과정과 복호화 과정의 주체를 상황에 따라 적절하게 결정함으로써 오류 정정 과정에 소요되는 시간과 비용을 감소시키고 보안성이 향상된 양자 암호 통신 방법 및 시스템이 개시될 수 있다.

[0007] 본 실시 예가 이루고자 하는 기술적 과제는 상기된 바와 같은 기술적 과제로 한정되지 않으며, 이하의 실시 예들로부터 또 다른 기술적 과제들이 유추될 수 있다.

### 과제의 해결 수단

[0008] 적어도 하나의 프로세서에 의해 수행되는 적어도 하나의 제1통신 장치와 적어도 하나의 제2통신 장치 사이의 양자 암호 통신 방법은, 상기 제1통신 장치가 광자의 위상이나 편광에 의해 랜덤하게 변조함으로써 생성된 제1정보열을 상기 제2통신 장치에 전송하면 상기 제2통신 장치가 상기 제1정보열에 기반하여 제2정보열을 생성하는 양자 통신 단계, 소정의 기준에 기반하여 선택된 오류 정정 모드 하에서 패리티 정보를 이용하여 상기 제1정보열과 제2정보열을 동일하도록 맞추는 후처리 단계를 포함하고, 상기 오류 정정 모드는, 상기 제1통신 장치가 제1패리티 정보를 부호화하여 상기 제2통신 장치에게 전송하면 상기 제2통신 장치가 상기 부호화된 제1패리티 정보를 복호화함으로써 상기 제2정보열을 상기 제1정보열과 동일하게 맞추는 제1오류 정정 모드와 상기 제2통신 장치가 제2패리티 정보를 부호화하여 상기 제1통신 장치에게 전송하면 상기 제1통신 장치가 상기 부호화된 제2패리티 정보를 복호화함으로써 상기 제1정보열을 상기 제2정보열과 동일하게 맞추는 제2오류 정정 모드 중 하나이고, 상기 소정의 기준은 상기 제1통신 장치와 상기 제2통신 장치 중 디텍터가 위치하지 않은 통신 장치가 상기 패리티 정보의 부호화를 수행하고, 상기 제1통신 장치와 상기 제2통신 장치 중 디텍터가 위치한 통신 장치가 상기 패리티 정보의 복호화를 수행하는 제1기준과 상기 패리티 정보에 대한 복호화 주체에 대한 정보가 포함된 시그널링 정보에 기반하여 상기 제1통신 장치와 상기 제2통신 장치 중 어느 하나가 상기 패리티 정보의 복호화를 수행하는 제2기준을 포함할 수 있다.

[0009] 적어도 하나의 제2통신 장치는 복수의 통신 장치들을 포함하고, 상기 제1통신 장치와 상기 복수의 통신 장치들 사이의 상기 후처리 단계는 상기 제1기준에 따라 수행될 수 있다.

[0010] 적어도 하나의 제2통신 장치는 복수의 통신 장치들을 포함하고, 상기 제1통신 장치와 상기 복수의 통신 장치들 사이의 상기 후처리 단계는 상기 제2기준에 따라 수행될 수 있다.

[0011] 적어도 하나의 프로세서에 의해 수행되는 적어도 하나의 제1통신 장치와 적어도 하나의 제2통신 장치 사이의 양

자 암호 통신 방법은, 상기 제1통신 장치가 광자의 위상이나 편광에 의해 랜덤하게 변조함으로써 생성된 제1정보열을 상기 제2통신 장치에 전송하면 상기 제2통신 장치가 상기 제1정보열에 기반하여 제2정보열을 생성하는 양자 통신 단계, 소정의 기준에 기반하여 선택된 오류 정정 모드 하에서 패리티 정보를 이용하여 상기 제1정보열과 제2정보열을 동일하도록 맞추는 후처리 단계를 포함하고, 상기 오류 정정 모드는, 상기 제1통신 장치가 제1패리티 정보를 부호화하여 상기 제2통신 장치에게 전송하면 상기 제2통신 장치가 상기 부호화된 제1패리티 정보를 복호화함으로써 상기 제2정보열을 상기 제1정보열과 동일하게 맞추는 제1오류 정정 모드와 상기 제2통신 장치가 제2패리티 정보를 부호화하여 상기 제1통신 장치에게 전송하면 상기 제1통신 장치가 상기 부호화된 제2패리티 정보를 복호화함으로써 상기 제1정보열을 상기 제2정보열과 동일하게 맞추는 제2오류 정정 모드 중 하나이고, 상기 소정의 기준은 도청자가 상기 제1통신 장치보다 상기 제2통신 장치에 더 가까이 위치하고 있으면 상기 오류 정정 모드는 상기 제1오류 정정 모드로 선택되고, 도청자가 상기 제2통신 장치보다 상기 제1통신 장치에 더 가까이 있으면 상기 오류 정정 모드는 상기 제2오류 정정 모드로 선택될 수 있다.

[0012] 양자 암호 통신 시스템은 광자의 위상이나 편광에 의해 랜덤하게 변조함으로써 생성된 제1정보열을 제2통신 장치에 전송하기 위한 제1통신 장치, 및 상기 수신된 제1정보열에 기반하여 제2정보열을 생성하기 위한 제2통신 장치를 포함하고, 소정의 기준에 기반하여 선택된 오류 정정 모드 하에서 패리티 정보를 이용하여 상기 제1정보열과 제2정보열을 동일하도록 맞추는 오류 정정 과정을 통해 양자키 분배가 수행되되, 상기 오류 정정 모드는, 상기 제1통신 장치가 제1패리티 정보를 부호화하여 상기 제2통신 장치에게 전송하면 상기 제2통신 장치가 상기 부호화된 제1패리티 정보를 복호화함으로써 상기 제2정보열을 상기 제1정보열과 동일하게 맞추는 제1오류 정정 모드와 상기 제2통신 장치가 제2패리티 정보를 부호화하여 상기 제1통신 장치에게 전송하면 상기 제1통신 장치가 상기 부호화된 제2패리티 정보를 복호화함으로써 상기 제1정보열을 상기 제2정보열과 동일하게 맞추는 제2오류 정정 모드 중 하나이고, 상기 소정의 기준은 상기 제1통신 장치와 상기 제2통신 장치 중 디텍터가 위치하지 않은 통신 장치가 상기 패리티 정보의 부호화를 수행하고, 상기 제1통신 장치와 상기 제2통신 장치 중 디텍터가 위치한 통신 장치가 상기 패리티 정보의 복호화를 수행하는 제1기준과 상기 패리티 정보에 대한 복호화 주체에 대한 정보가 포함된 시그널링 정보에 기반하여 상기 제1통신 장치와 상기 제2통신 장치 중 어느 하나가 상기 패리티 정보의 복호화를 수행하는 제2기준을 포함할 수 있다.

[0013] 광자의 위상이나 편광에 의해 랜덤하게 변조함으로써 생성된 제1정보열을 제2통신 장치에 전송하기 위한 제1통신 장치, 및 상기 수신된 제1정보열에 기반하여 제2정보열을 생성하기 위한 제2통신 장치를 포함하고, 소정의 기준에 기반하여 선택된 오류 정정 모드 하에서 패리티 정보를 이용하여 상기 제1정보열과 제2정보열을 동일하도록 맞추는 오류 정정 과정을 통해 양자키 분배가 수행되되, 상기 오류 정정 모드는, 상기 제1통신 장치가 제1패리티 정보를 부호화하여 상기 제2통신 장치에게 전송하면 상기 제2통신 장치가 상기 부호화된 제1패리티 정보를 복호화함으로써 상기 제2정보열을 상기 제1정보열과 동일하게 맞추는 제1오류 정정 모드와 상기 제2통신 장치가 제2패리티 정보를 부호화하여 상기 제1통신 장치에게 전송하면 상기 제1통신 장치가 상기 부호화된 제2패리티 정보를 복호화함으로써 상기 제1정보열을 상기 제2정보열과 동일하게 맞추는 제2오류 정정 모드 중 하나이고, 상기 소정의 기준은 도청자가 상기 제1통신 장치보다 상기 제2통신 장치에 더 가까이 위치하고 있으면 상기 오류 정정 모드는 상기 제1오류 정정 모드로 선택되고, 도청자가 상기 제2통신 장치보다 상기 제1통신 장치에 더 가까이 있으면 상기 오류 정정 모드는 상기 제2오류 정정 모드로 선택될 수 있다.

### 발명의 효과

[0014] 오류 정정 과정에서 필요한 부호화 과정과 복호화 과정의 주체를 상황에 따라 적절하게 결정함으로써 오류 정정 과정에 소요되는 시간과 비용을 감소시키고 보안성이 향상된 양자 암호 통신 방법 및 시스템이 개시될 수 있다.

### 도면의 간단한 설명

[0015] 도1은 일 실시 예에 따라, 양자 암호 통신 방법의 흐름도를 나타낸다.

도2는 일 실시 예에 따라, 양자 암호 통신 시스템을 나타낸다.

도3은 일 실시 예에 따라, 일반적인 이동 통신에서 수행되는 정보 보정 과정을 나타낸다.

도4는 일 실시 예에 따라, 제1오류 정정 모드를 나타낸다.

도5는 일 실시 예에 따라, 제2오류 정정 모드를 나타낸다.

도6은 일 실시 예에 따라, 일방향 방식에 기반한 양자 암호 통신을 나타낸다.

도7은 일 실시 예에 따라, 양방향 방식에 기반한 양자 암호 통신을 나타낸다.

도8은 일 실시 예에 따라, 스마트폰과 ATM 기기 사이의 양자 암호 통신을 나타낸다.

도9는 일 실시 예에 따라, 도청자 Eve가 Alice 근처에 있는 상태를 나타낸다.

도10은 일 실시 예에 따라, 도청자 Eve가 Bob 근처에 있는 상태를 나타낸다.

도11은 일 실시 예에 따라, 패리티 정보의 부호화와 패리티 정보의 복호화의 주체를 구분하기 위한 시그널링 정보를 나타낸다.

도12는 일 실시 예에 따라, 일대다 양자 암호 통신 시스템을 나타낸다.

도13은 일 실시 예에 따라, 시그널링 정보를 사용하지 않고 기본 설정을 사용하여 패리티 정보의 복호화를 수행하는 것을 나타낸다.

도14는 일 실시 예에 따라, 시그널링 정보를 하나의 비트만 사용하여 패리티 정보의 복호화를 수행하는 것을 나타낸다.

도15는 일 실시 예에 따라, 추가 비트를 사용하여 패리티 정보 복호화의 주체를 개별적으로 지정함으로써 패리티 정보의 복호화를 수행하는 것을 나타낸다.

도16은 일 실시 예에 따라, 다대다 양자 암호 통신 시스템을 나타낸다.

### 발명을 실시하기 위한 구체적인 내용

[0016] 아래에서, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자들(이하, 통상의 기술자들)이 본 발명을 용이하게 실시할 수 있도록, 첨부되는 도면들을 참조하여 몇몇 실시 예가 명확하고 상세하게 설명될 것이다.

[0017] 이하, 도2를 참조하여 상술한 Alice와 Bob은 각각 정보열의 송신자와 수신자이다. Alice와 Bob은 각각 Alice가 보유한 제1통신 장치와 Bob이 보유한 제2통신 장치를 나타낼 수 있다. 통신 장치는 전화기, 컴퓨터, 랩 탑, 모바일 장치, 서버 장치, 클라우드 장치, 위성 장치, AP(Access Point), 가전 제품, 상업용 전자 장치 등 통신을 수행할 수 있는 어떠한 형태의 전자 장치도 포함할 수 있다. 예로서, Alice는 스마트폰이고 Bob은 ATM기기일 수 있다.

[0018] 통신에서 정보 보정 내지 오류 정정은 송신자와 수신자 사이에 동일한 정보를 가질 수 있도록 정보를 보정하는 과정을 의미한다. 도3은 일 실시 예에 따라, 일반적인 이동 통신에서 수행되는 정보 보정 과정을 나타낸다. 도3을 참조하면, 일반적인 이동 통신에 있어서, 오류 정정 과정은 송신자만 알고 있는 정보열에 부가 정보(예로서, 패리티 비트(parity bit) 내지 신드롬(syndrome))을 부가함으로써, 통신 채널을 통해 정보열(실제 데이터)과 부가 정보(예 : 패리티 비트)를 전송하고 수신자는 수신한 정보들을 이용하여 송신자가 가지고 있는 정보열과 동일하도록 자신의 정보열을 재구성하는 방식이다.

[0019] 이러한 오류 정정은 양자 암호 통신 시스템(100)에서도 유사하게 수행된다. 이하, 오류 정정을 위해 사용되는 부가 정보를 "오류 정정 부호"라고 하고, "패리티 정보"가 오류 정정 부호의 대표적인 실시 예로 기술되나 오류 정정 부호는 패리티 정보로 한정되지 않는다. 양자 암호 통신 시스템(100)에 있어서, 이러한 정보 보정은 양자 통신 단계(도1의 단계 S10)가 종료된 후 송신자와 수신자가 가지고 있는 정보열(제1정보열 내지 제2정보열)에 대한 추가적인 정보 전송(즉, 패리티 정보)을 통해 수행될 수 있다. 즉, 일반적인 이동 통신과 달리 양자 암호 통신에서 오류 정정 부호는 양자 통신 단계가 완료된 이후인 후처리 단계에서 활용되고, 이미 송신자와 수신자가 자신의 정보열을 각각 가지고 있는 상태에서 오류 정정 과정이 수행될 수 있다. 따라서, 오류 정정 과정은 통신 채널이 도청자에 의해 도청되고 있다는 전제 하에서 수행될 수 있다. 즉, 통신 채널이 도청이 되고 있기 때문에 통신 채널을 통해 전송되는 정보는 최소화될 필요가 있다.

[0020] 도4는 일 실시 예에 따라, Alice가 패리티 정보의 부호화를 수행하고 Bob이 패리티 정보의 복호화를 수행하는 제1오류 정정 모드를 나타낸다. 도5는 일 실시 예에 따라, Bob이 패리티 정보의 부호화를 수행하고 Alice가 패리티 정보의 복호화를 수행하는 제2오류 정정 모드를 나타낸다.

[0021] 패리티 정보는 송신자에 의해 수행되는 부호화 과정과 수신자에 의해 수행되는 복호화 과정을 거친다. 즉, 패리티 정보의 송신자가 패리티 정보를 부호화해서 통신의 상대방에게 송신하면 통신의 상대방, 즉 패리티 정보의 수신자는 수신된 패리티 정보를 복호화할 수 있다. 일반적으로 복호화 과정에 소요되는 시간이 부호화 과정에 소요되는 시간에 비해 오래 걸리고 연산도가 복잡하다. 일반적인 이동 통신에서는 정보의 송신자Alice가 패리티

정보의 부호화를 수행하고 정보의 수신자Bob가 패리티 정보의 복호화를 수행한다.

- [0022] 다만, 양자 암호 통신 시스템(100)에서는 (양자 암호 단계가 완료된 이후에는) 송신자 Alice와 수신자 Bob이 각자의 정보열을 이미 보유하고 있다. 따라서, 양자 통신 단계(S10)에서 Alice는 정보열의 송신자이고 Bob은 정보열의 수신자이나 이와는 별개로 후처리 단계(S20)에서 Alice와 Bob은 패리티 정보의 수신자 또는 송신자가 각각 될 수 있다.
- [0023] 일 실시 예에 따라, Alice가 패리티 정보에 대한 부호화를 수행한 후 부호화된 패리티 정보를 통신 채널을 통해 Bob에게 전송하고, Bob은 수신한 패리티 정보와 자신이 기 보유한 제2정보열을 이용해 복호화를 수행함으로써 제2정보열을 제1정보열과 동일하게 맞출 수 있다. Bob은 복호화 결과 또는 추가적으로 필요한 정보에 대한 피드백 신호를 Alice에게 송신할 수 있다. 이를 제1오류 정정 모드로 지칭할 수 있다(도4 참조).
- [0024] 다른 실시 예에 따라, Bob이 패리티 정보에 대한 부호화를 수행한 후 부호화된 패리티를 통신 채널을 통해 Alice에게 전송하고, Alice는 수신한 패리티 정보와 자신이 기 보유한 제1정보열을 이용해 복호화를 수행함으로써 제1정보열을 제2정보열과 동일하게 맞출 수 있다. Alice는 복호화 결과 또는 추가적으로 필요한 정보에 대한 피드백 신호를 Bob에게 송신할 수 있다. 이를 제2오류 정정 모드로 지칭할 수 있다(도5 참조). 도5와 도6을 참조하면, 양자 암호 통신에서 양자 통신 단계가 완료된 이후에 패리티 정보를 송수신하는 것은 반드시 정보열의 송신자가 패리티 정보를 부호화하여 전송하고 정보열의 수신자가 수신한 패리티를 복호화하여야 하는 것은 아니다.
- [0025] 다만, 제1오류 정정 모드에서 전송되는 패리티 정보는 Alice가 가지고 있는 제1정보열에 기반하여 생성되고, 제2오류 정정 모드에서 전송되는 패리티 정보는 Bob이 가지고 있는 제2정보열에 기반하여 생성되기 때문에 오류 정정 모드에 따라 생성되는 패리티 정보는 서로 다를 수 있다(도4의 제1패리티와 도5의 제2패리티는 서로 상이).
- [0026] 소정의 기준에 기반하여 제1오류 정정 모드와 제2오류 정정 모드 중 하나가 결정될 수 있으며 이하, 패리티 정보의 부호화와 복호화의 수행 주체(Alice와 Bob)를 결정하는 소정의 기준이 개시된다.
- [0027] 첫 번째 기준(제1 기준)은 복호화 과정의 연산도가 높음을 고려하여 하드웨어 장치의 성능이 좋은 주체가 패리티 정보의 복호화를 수행하도록 하는 것이다.
- [0028] 양자 암호 통신에서 양자 통신 단계의 수행은 크게 일방향(one-way) 방식과 양방향(two-way 또는 plug and play) 방식으로 구분될 수 있다. 도6을 참조하면, 일방향 방식 하에서 정보를 실을 수 있는 광자를 생성하기 위한 레이저(laser)가 송신자 Alice에게 위치하고, 광자를 검출하기 위한 디텍터(detector)는 수신자 Bob에게 위치할 수 있다. 이에 반해, 도7을 참조하면, 양방향 방식 하에서 송신자 Alice 또는 수신자 Bob 중 어느 한쪽(도7에서는 Bob)에 부피가 크고 비용이 비싼 레이저와 디텍터를 동시에 위치시킬 수 있다. 첫 번째 기준에 따라, Alice와 Bob 중 하드웨어 장치의 성능이 더 우수한 주체가 패리티 정보의 복호화 과정을 수행할 수 있다.
- [0029] 양방향 방식은 전송 속도 저하에도 불구하고 광섬유를 통한 양자 키 분배 시에 발생하는 편광의 변화나 경로의 흔들림을 보상하기 위해 사용되는데, 예로서, 스마트폰과 같은 휴대용 단말기와 은행의 ATM기기 사이에 양자 암호 통신이 수행되는 경우 휴대용 단말기는 메모리와 프로세서의 성능에 한계가 존재하는 경량화된 장치이므로 ATM기기에 레이저와 디텍터가 위치할 수 있다.
- [0030] 일 실시 예에 따라, Alice와 Bob 중 디텍터가 위치한 주체가 하드웨어 장치의 성능이 더 우수한 것으로 판단될 수 있다. Alice가 스마트폰이고 Bob이 레이저와 디텍터가 위치한 ATM기기일 경우 패리티 정보의 복호화는 Bob에서 수행되고 부호화는 Alice에 의해 수행될 수 있다(도8 참조).
- [0031] 두 번째 기준(제2기준)은 Alice와 Bob 중 도청자와 더 가까이 있는 주체가 패리티 정보 복호화를 수행하고 나머지 주체가 패리티 정보 부호화를 수행하도록 하는 것이다. 통신 채널(유선 또는 무선을 불문함)은 일반적으로 전송ロス(loss)로 인해 송신자 근처에서는 신호의 세기가 크지만 수신자는 감쇄된 신호를 수신할 수 있다. 만약, 도청자 Eve가 Alice와 Bob중 어느 하나에 가까이 위치하고 있다면 도청자 Eve는 가까이 위치한 주체로부터 패리티 신호를 도청할 수 있다. 만약, 패리티 정보의 송신자가 Alice이고 도청자 Eve가 Alice 근처에 있다면(도9 참조) 도청자 Eve는 Bob에 비해 패리티 신호를 강하게 수신할 수 있고 도청자 Eve가 Bob 근처에 있을 때(도10 참조) 비해 도청 정보가 많아질 수 있다. 즉, 도청자 Eve가 Alice 근처에 있다면 Bob 이 패리티 정보의 송신자로 결정됨으로써 도청자 Eve의 도청 정보량이 감소될 수 있다. 결론적으로, 도청자가 상대적으로 가까이 위치한 주체가 패리티 정보 복호화를 수행하고 멀리 있는 주체가 패리티 정보 부호화를 수행하도록 결정될 수 있다.

- [0032] 두 번째 기준의 예시로서, 지상국과 위성 사이의 양자 암호 통신에서 위성이 장비 등의 업데이트가 힘들다는 것을 고려하여 지상국에 레이저와 디텍터를 위치시키되 도청용 위성이 통신 대상 위성의 주변에 있을 수 있으므로 지상국에서 패리티 부호화를 수행하고 위성이 패리티 정보의 복호화를 수행하도록 할 수 있다. 이런 상황에서는 첫 번째 기준에 따르면 디텍터가 위치한 지상국이 패리티 정보의 복호화를 수행해야 하지만 두 번째 기준에 따르면 위성이 패리티 정보의 복호화를 수행할 수 있다. 즉, 도청자의 위치가 비교적 명확하다면 두 번째 기준이 첫 번째 기준보다 우선할 수 있으며 두 번째 기준 적용시에는 패리티 정보 복호화의 수행 주체를 결정하기 위해 도청자의 위치가 변경될 수 있음을 고려하여야 한다.
- [0033] 세 번째 기준(제3기준)은 상황에 따라 패리티 정보의 복호화 주체를 양자 암호 통신 시스템(100) 내지 양자 암호 통신 시스템(100)의 통신 주체 또는 운영자가 직접 지정하는 것이다. 이러한 실시 예에서, 미리 약속한 시그널링 정보에 대한 프로토콜을 지정해놓고 정해놓은 시그널링 정보에 따라 패리티 정보의 복호화 주체와 부호화 주체가 결정될 수 있다. 이러한 시그널링 정보는 Alice 와 Bob 사이에 한번의 패리티 정보의 전송으로 오류 정정 과정이 종료되는 것이 아니라 추가적인 패리티의 전송이 더 수행될 수도 있기 때문에 더욱 중요하다. 예를 들어, Alice 가 패리티 정보를 부호화하여 Bob 이 패리티를 수신하여 복호화하고, 복호화 주체인 Bob이 부호화를 수행하여 추가적인 패리티 정보를 생성하고 추가적인 패리티 정보가 다시 Alice 에게 전송될 수 있다. Alice 는 수신한 추가적인 패리티 정보를 다시 복호화할 수 있다. 즉, 최초의 패리티 정보의 부호화 주체가 누가 될 것인지를 나타내는 시그널링 정보가 필요할 수 있다.
- [0034] 도11은 일 실시 예에 따라, 패리티 정보의 부호화와 패리티 정보의 복호화의 주체를 구분하기 위한 시그널링 정보를 나타낸다.
- [0035] 시그널링 정보는 송신자와 수신자 중 (최초의) 패리티 복호화(또는, 부호화)의 주체가 누구인지를 나타내기 위한 정보이다. 만약, Alice와 Bob 사이에 시그널링 정보가 전송되지 않는다면 디텍터를 가지고 있는 주체가 패리티 복호화를 수행하도록 기본 설정될 수 있다(제1기준).
- [0036] 시그널링 정보는 크기  $m$ ( $m$ 은 정수)의 비트열로 구성될 수 있다.  $m$ 이 1이면 시그널링 정보는 1bit크기로 구성되고  $m$ 이 2이면 시그널링 정보는 2bit크기로 구성될 수 있다.
- [0037] 시그널링 정보가 전송이 된다면, 시그널링 정보가 '0'이라면 디텍터를 가지고 있지 않은 주체에서 패리티 정보의 복호화가 수행될 수 있다. 시그널링 정보가 '1'이라면 패리티 정보의 복호화를 수행하기 위한 주체가 양자 암호 통신 시스템(100)에 의해 개별 지정될 수 있다. 즉, 양자 암호 통신 시스템(100)은 Alice 와 Bob 중 어느 하나에게 패리티 정보의 복호화를 수행하도록 지정할 수 있으며 이러한 실시 예에서, 시그널링 정보는 추가 비트인 1bit를 더 포함함으로써 총 2bit 크기가 되고 시그널링 정보에 따라 패리티 복호화를 수행할 주체가 지정될 수 있다. 예를 들어, 추가 비트의 값이 '0'이면 Alice 가 패리티 정보의 복호화를 수행하고 '1'이면 Bob이 패리티 정보의 복호화를 수행할 수 있다.
- [0038] 일 실시 예에 따라, 시그널링 정보는 기본적으로 2bit 크기로 구성될 수 있다. 예를 들어, 시그널링 정보가 '00'이면 디텍터를 가지고 있는 주체가 패리티 정보 복호화를 수행하고 '01'이면 디텍터를 가지고 있지 않은 주체가 패리티 정보 복호화를 수행할 수 있다. 시그널링 정보가 '10'이면 Alice 와 Bob 모두 부호화 또는 복호화가 가능하다는 것을 나타낼 수 있다. 시그널링 정보가 '11'이면 최초의 패리티 정보의 부호화 내지 복호화를 수행하는 주체가 Alice 와 Bob 중 하나로 특정될 수 있다.
- [0039] 예를 들어, Alice 가 패리티 정보를 최초로 부호화하여 Bob 이 패리티를 수신하여 복호화하고, 복호화 주체인 Bob이 부호화를 수행하여 추가적인 패리티 정보를 생성하고 추가적인 패리티 정보가 다시 Alice 에게 전송될 수 있다. Alice는 수신한 추가적인 패리티 정보를 다시 복호화할 수 있다. 즉, 한 번의 패리티 전송으로 오류 정정 과정이 종료되지 않은 상황을 가정하여 시그널링 정보를 2bit로 구성할 수 있다. 일 실시 예에 따라, 2bit 크기의 시그널링 정보의 상위 비트가 특정 값(예를 들어, 1)이면 한 번의 패리티 전송으로 오류 정정 과정이 종료되지 않은 상황을 의미할 수 있고, 하위 비트의 값에 기반하여 Alice와 Bob 중 어느 주체가 먼저 부호화 내지 복호화를 수행할지 결정될 수 있다.
- [0040] 시그널링 정보는 양자 암호 통신 방법이 수행되는 동안 Alice 와 Bob 사이에 주기적 또는 비주기적으로 전송될 수 있다. 예를 들어, 양자 키 분배가 수행되는 경우 무조건 해당 시그널링을 전송하거나 양자 통신 단계(도1의 S10) 수행 횟수에 따른 주기적 전송, 일정 시간동안 주기적으로 전송할 수도 있다.
- [0041] 상술한 시그널링 정보의 크기나 규칙은 얼마든지 변형 가능하고 Alice 와 Bob 사이의 약속 내지는 양자 통신 시스템(100)의 프로토콜에 따라 수많은 실시 예가 생길 수 있음을 당업자는 이해할 수 있을 것이다. 따라서, 본

발명은 도11을 참조하여 상술한 실시 예로 한정되지 않음을 이해하여야 한다. 또한, 도11을 참조하여 상술한 실시 예는 일대일 양자 암호 통신 시스템에 관한 것으로서 이는 일대다, 다대일, 또는 다대다 양자 암호 통신 시스템에도 동일하게 적용될 수 있다.

[0042] 도12는 일 실시 예에 따라, 일대다 양자 암호 통신 시스템을 나타낸다. 일대다 양자 암호 통신은 하나의 송신자(Alice)가 복수의 수신자들( $Bob_1, Bob_2, \dots, Bob_N$ )과 통신하는 방식이다( $N$ 은 양의 정수).

[0043] 일대다 양자 암호 통신 시스템(200)은 Alice 와  $Bob_1$  사이의 일대일 양자 암호 통신, Alice 와  $Bob_2$  사이의 일대일 양자 암호 통신, ..., Alice와  $Bob_N$ 과의 일대일 양자 암호 통신으로 구성될 수 있다. 즉, 일대다 양자 암호 통신 시스템(200)은 복수의 일대일 양자 암호 통신들로 구성될 수 있다.

[0044] 일대다 양자 암호 통신 시스템(200)에서, 패리티 정보 복호화 주체를 나타내는 시그널링 정보는  $m*N$  크기의 비트가 사용될 수 있다.  $m$ 비트는 일대일 통신에서의 시그널링 정보의 크기이고  $N$ 은 일대일 양자 암호 통신의 개수이다. 즉, 일대다 양자 암호 통신 시스템(200)은 통신 채널( $CH_1$ )을 통해 수행되는 Alice와  $Bob_1$  사이의 일대일 양자 암호 통신, 통신 채널( $CH_2$ )을 통해 수행되는 Alice와  $Bob_2$  사이의 일대일 양자 암호 통신, ..., 및 통신 채널( $CH_N$ )을 통해 수행되는 Alice와  $Bob_N$  사이의 일대일 양자 암호 통신으로 구성되므로 각 통신 채널을 통한 일대일 양자 암호 통신은 도11을 참조하여 상술한 시그널링 정보에 대한 내용이 동일하게 적용될 수 있다.

[0045] 일 실시 예에 따라, 시그널링 정보를 위해 전송되는 비트량을 감소시키기 위해 일대다 양자 암호 통신에 참여하는 모든 주체 내지 적어도 일부의 주체들은 시그널링 정보를 사용하지 않고 기본 설정(즉, 디텍터를 가지고 있는 주체가 패리티 정보의 복호화를 수행)을 사용할 수 있도록 설정될 수 있다. 도13은 일 실시 예에 따라, 시그널링 정보를 사용하지 않고 기본 설정을 사용하여 패리티 정보의 복호화를 수행하는 것을 나타낸다(수신자들( $Bob_1, Bob_2, \dots, Bob_N$ ) 각각에 디텍터가 위치하는 것으로 가정함).

[0046] 일대다 양자 암호 통신 시스템(200) 전체에 패리티 정보 복호화의 주체를 결정하는 기준을 통일시킬 수 있다. 이러한 실시 예에서,  $m*N$  비트를 사용하는 대신에 하나의 비트만으로 패리티 정보 복호화를 수행할 주체가 결정될 수 있다. 일 실시 예에 따라, 일대다 양자 암호 통신 시스템(200) 전체에서 시그널링 정보는 오로지 1bit 크기로만 구성되고 송신자 Alice와 수신자들 그룹( $Bob_1, Bob_2, \dots, Bob_N$ ) 중 어느 하나가 패리티 정보의 복호화 주체로 결정될 수 있다. 예를 들어, 시그널링 정보가 '0'이면 송신자 Alice가 부호화, 수신자들 그룹( $Bob_1, Bob_2, \dots, Bob_N$ )이 복호화를 수행할 수 있다. 시그널링 정보가 '1'이면 송신자 Alice가 복호화, 수신자들 그룹( $Bob_1, Bob_2, \dots, Bob_N$ )이 부호화를 수행할 수 있다. 도14는 일 실시 예에 따라, 시그널링 정보를 하나의 비트만 사용하여 패리티 정보의 복호화를 수행하는 것을 나타낸다. 일 실시 예에 따라, 시그널링 정보는 2bit 크기로 구성되어 상위 비트에 패리티 정보 복호화의 주체를 결정하는 기준을 통일시킨다는 것을 나타내는 비트 값이 위치하고 하위 비트에 패리티 정보 복호화의 주체를 특정하는 비트 값이 위치할 수도 있으나 이는 자유롭게 구성할 수 있으므로 제한되지 않는다.

[0047] 일 실시 예에 따라, 일대다 양자 암호 통신 시스템(200)을 구성하는 일대일 통신들 중 일부는 패리티 정보 복호화의 주체를 결정하는 기준을 통일시키고 나머지는 개별적으로 패리티 정보 복호화 주체를 지정하도록 할 수도 있다. 패리티 정보의 복호화 주체를 개별적으로 지정하기 위해 시그널링 정보는 추가 비트를 더 필요로 할 수 있다. 도15는 일 실시 예에 따라, 추가 비트를 사용하여 패리티 정보 복호화의 주체를 개별적으로 지정함으로써 패리티 정보의 복호화를 수행하는 것을 나타낸다. 추가 비트를 사용하면 시그널링 정보의 크기는 증가하게 된다.

[0048] 다대일 양자 암호 통신은 복수의 송신자들( $Alice_1, Alice_2, \dots, Alice_N$ )이 하나의 수신자( $Bob$ )와 통신하는 방식이다( $N$ 은 양의 정수). 다대일 양자 암호 통신은 일대다 양자 암호 통신과 반대 구조이기 때문에 일대다 양자 암호 통신에 관하여 상술된 내용은 다대일 양자 암호 통신에도 동일하게 적용될 수 있으므로 상세한 설명은 생략한다.

[0049] 도16은 일 실시 예에 따라, 다대다 양자 암호 통신 시스템을 나타낸다.

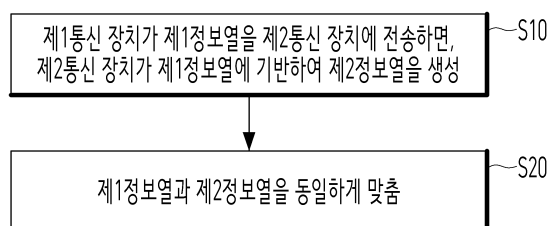
[0050] 다대다 양자 암호 통신은 복수의 송신자들( $Alice_1, Alice_2, \dots, Alice_N$ )이 복수의 수신자들( $Bob_1, Bob_2, \dots, Bob_K$ )와 통신하는 방식이다( $N$ 과  $K$ 는 양의 정수). 예로서, 다대다 양자 암호 통신 시스템(300)은  $Alice_1$ 과  $Bob_1$

사이의 일대일 통신, Alice<sub>1</sub>과 Bob<sub>2</sub> 사이의 일대일 통신, Alice<sub>1</sub>과 Bob<sub>N</sub>사이의 일대일 통신, Alice<sub>2</sub>와 Bob<sub>1</sub> 사이의 일대일 통신, Alice<sub>2</sub>와 Bob<sub>2</sub> 사이의 일대일 통신, Alice<sub>2</sub>와 Bob<sub>N</sub>사이의 일대일 통신으로 구성될 수 있다. 즉, 다대다 양자 암호 통신 시스템(300)은 N\*K 개의 일대일 양자 암호 통신들로 구성될 수 있다.

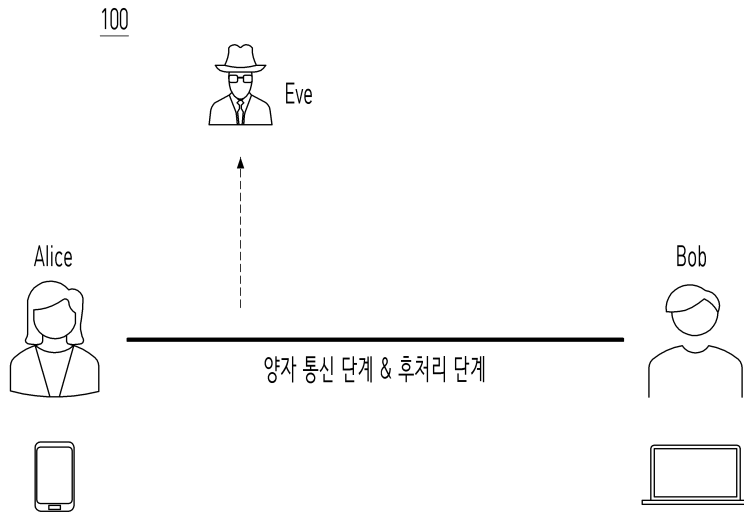
- [0051] 각 통신 채널을 통한 일대일 양자 암호 통신은 도11을 참조하여 상술한 시그널링 정보에 대한 내용이 동일하게 적용될 수 있다. 다대다 양자 암호 통신 시스템(300)에서, 패리티 정보 복호화 주체를 나타내는 시그널링 정보는 m\*N\*K 크기의 비트로 나타낼 수 있다. m비트는 일대일 통신에서의 시그널링 정보의 크기이다.
- [0052] 일 실시 예에 따라, 다대다 양자 암호 통신 시스템(300)에 참여하는 모든 주체 내지 일부의 주체들은 시그널링 정보를 사용하지 않고 기본 설정(즉, 디텍터를 가지고 있는 주체가 패리티 복호화를 수행)을 사용할 수 있도록 설정될 수 있다.
- [0053] 일 실시 예에 따라, 다대다 양자 암호 통신 시스템(300) 전체에 대한 패리티 정보 복호화의 주체를 결정하는 기준이 통일될 수 있다. 또는, 다대다 양자 암호 통신 시스템(300)에서 송신자 별로 그룹을 나누고(예로서, Alice<sub>1</sub>과 수신자들(Bob<sub>1</sub>, Bob<sub>2</sub>, ..., Bob<sub>K</sub>) 사이의 제1통신 그룹 및 Alice<sub>2</sub>와 수신자들(Bob<sub>1</sub>, Bob<sub>2</sub>, ..., Bob<sub>K</sub>) 사이의 제2통신 그룹), 각 그룹 별로 패리티 정보 복호화의 주체를 결정하는 기준을 다르게 적용하되 하나의 그룹에서는 기준을 통일시킬 수 있다. 또는, 다대다 양자 암호 통신 시스템(300)에서 수신자 별로 그룹을 나누고(예로서, Bob<sub>1</sub>과 송신자들(Alice<sub>1</sub>, Alice<sub>2</sub>) 사이의 제1통신 그룹, Bob<sub>2</sub>와 송신자들(Alice<sub>1</sub>, Alice<sub>2</sub>) 사이의 제2통신 그룹, 및 Bob<sub>3</sub>과 송신자들(Alice<sub>1</sub>, Alice<sub>2</sub>) 사이의 제3통신 그룹) 각 그룹 별로 패리티 정보 복호화의 주체를 결정하는 기준을 다르게 적용하되 하나의 그룹에서는 기준을 통일시킬 수 있다.
- [0054] 일 실시 예에 따라, 다대다 양자 암호 통신 시스템(300)을 구성하는 일대일 통신들 중 일부는 패리티 정보 복호화의 주체를 결정하는 기준을 통일시키고 나머지는 개별적으로 패리티 복호화 주체를 지정하도록 할 수도 있다. 개별적으로 패리티 복호화 주체를 지정하기 위해 시그널링 정보는 복호화 주체를 특정하기 위한 추가 비트를 더 필요로 할 수 있다.
- [0055] 일 실시 예에 따라, 상술한 시그널링 정보는 5G, LTE-A, LTE, Wi-Fi 등의 물리 하향 링크 제어 채널(Physical Downlink Control Channel, PDCCH), 향상된 물리 하향 링크 제어 채널(Enhanced PDCCH), 물리 하향 링크 공유 채널(Physical Downlink Control Channel, PDSCH), Cell-특정 상위 계층 시그널링(Cell specific high-layer signaling), UE-특정 상위 계층 시그널링(UE specific high-layer signaling)등의 방식을 이용하여 송신자와 수신자 사이에 전송될 수 있다.
- [0056] 일 실시 예에 따라, 시그널링 정보는 분배된 양자 키 중 일부 정보일 수 있다. 예로서, 도1의 단계 S10 이후 Bob에 의해 생성된 제2정보열에 시그널링 정보가 포함될 수 있으나 이에 제한되지 않는다.
- [0057] 설명들은 본 발명을 구현하기 위한 예시적인 구성들 및 동작들을 제공하도록 의도된다. 본 발명의 기술 사상은 위에서 설명된 실시 예들뿐만 아니라, 위 실시 예들을 단순히 변경하거나 수정하여 얻어질 수 있는 구현들도 포함할 것이다. 또한, 본 발명의 기술 사상은 위에서 설명된 실시 예들을 앞으로 용이하게 변경하거나 수정하여 달성될 수 있는 구현들도 포함할 것이다.

## 도면

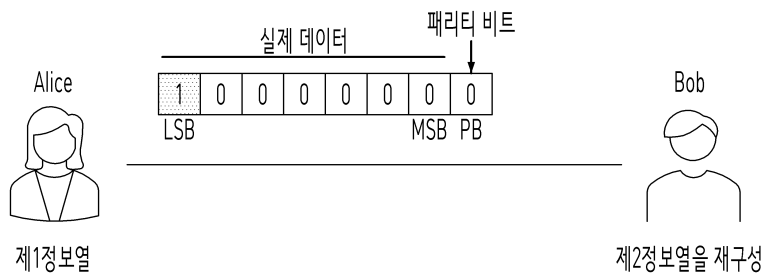
### 도면1



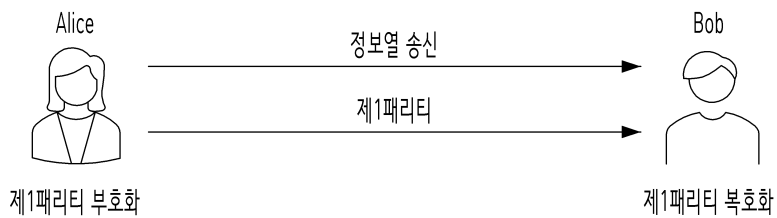
도면2



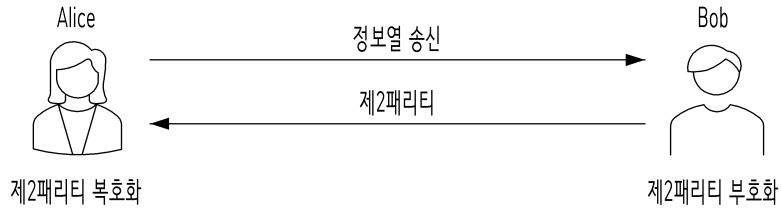
도면3



도면4



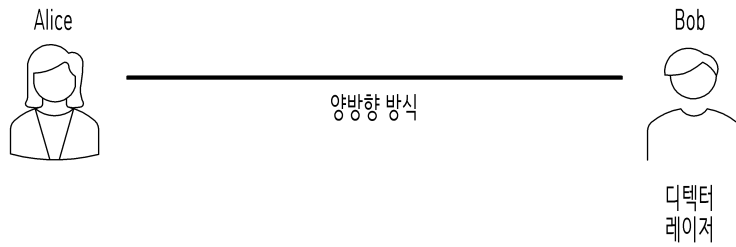
도면5



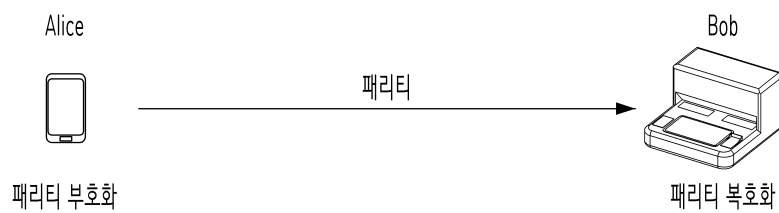
도면6



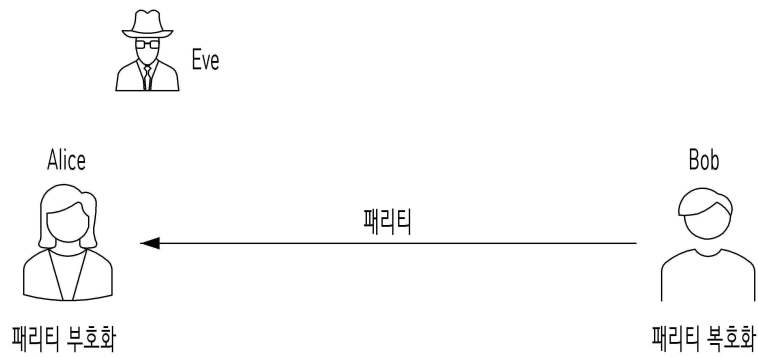
도면7



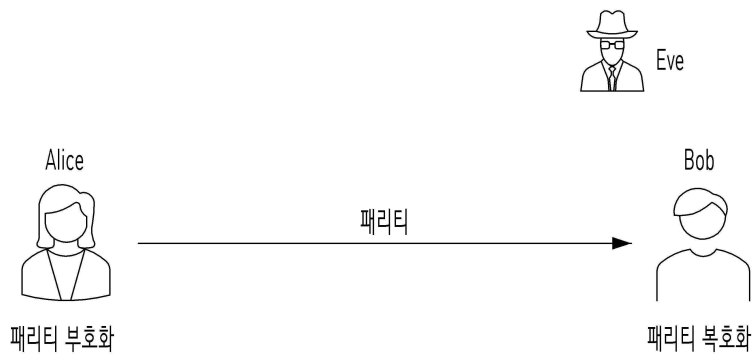
도면8



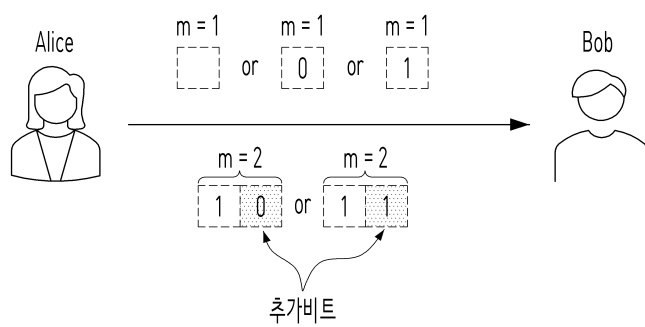
도면9



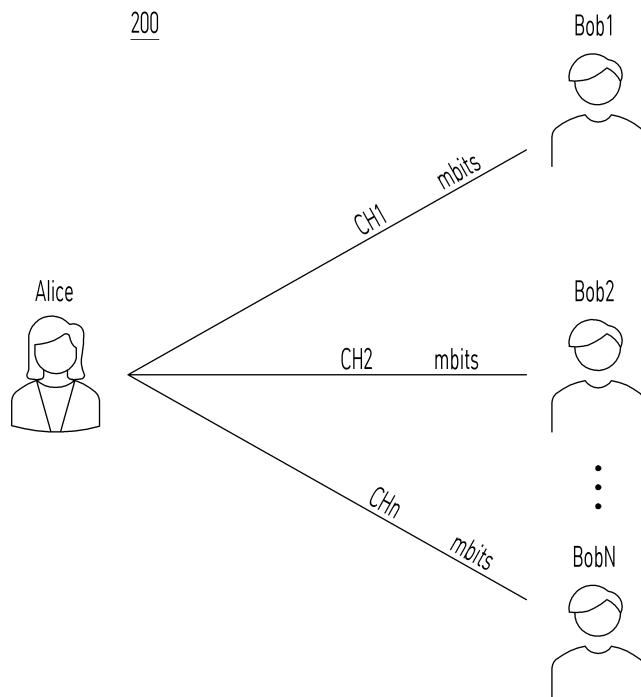
도면10



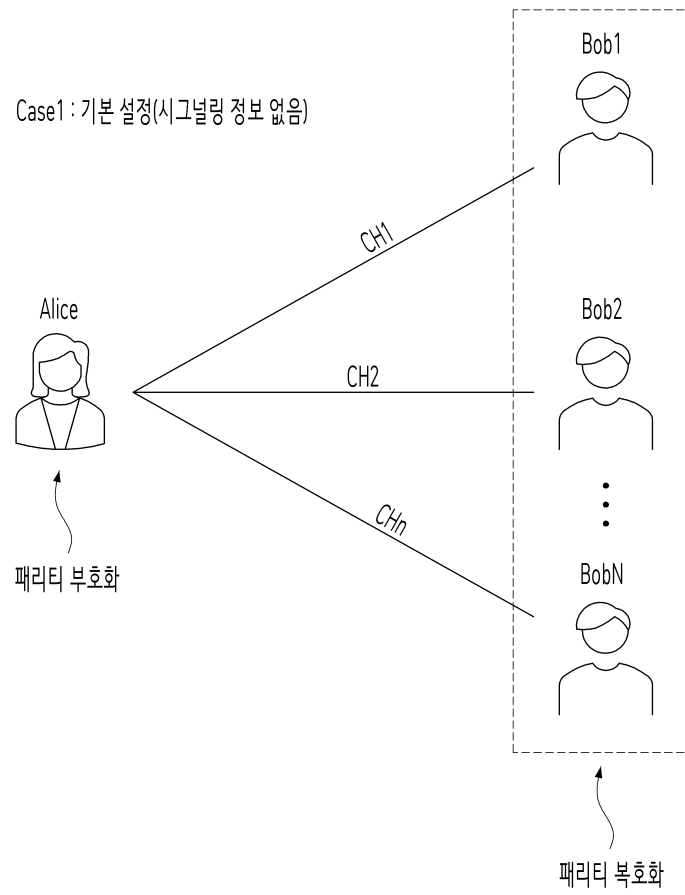
도면11



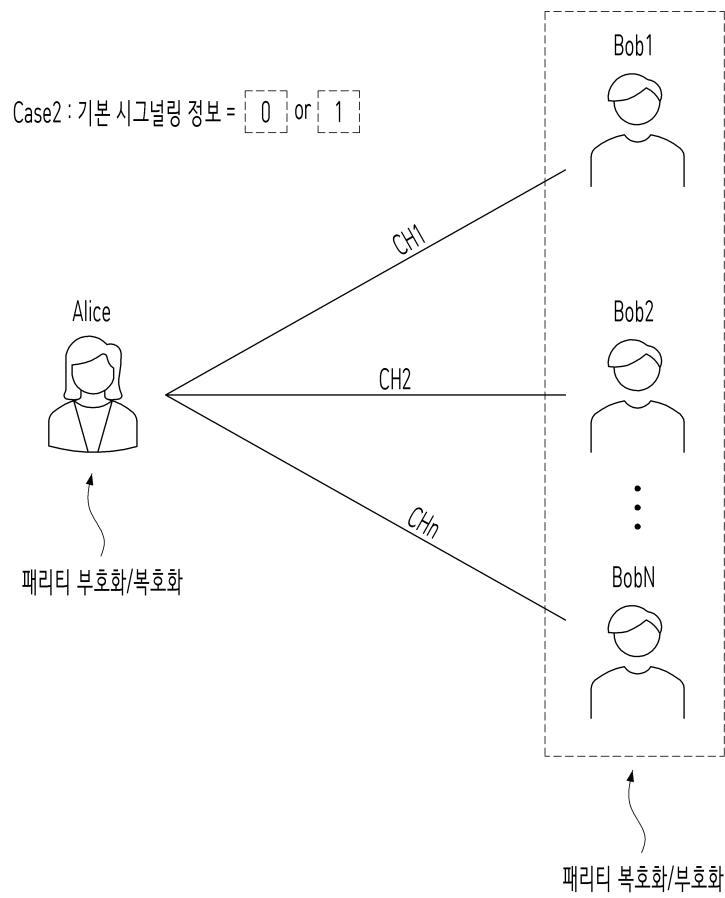
도면12



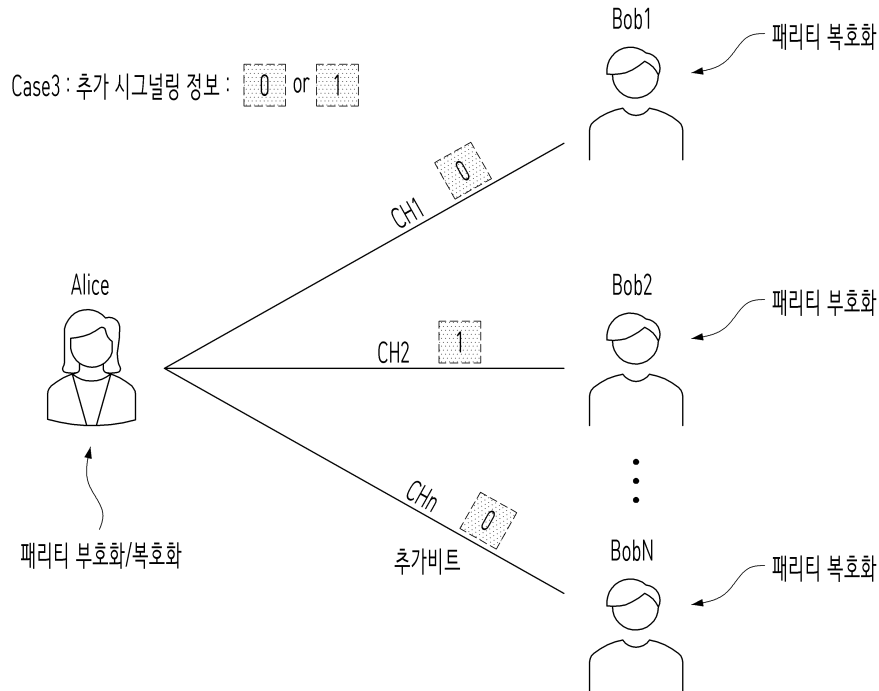
도면13



도면14



도면15



도면16

300

Case1 : 기본 설정(시그널링 정보 없음)

Case2 : 기본 시그널링 정보 : 0 or 1

Case3 : 추가 시그널링 정보 : 0 or 1

