



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0071634
(43) 공개일자 2018년06월28일

(51) 국제특허분류(Int. Cl.)

H04L 9/08 (2006.01)

(52) CPC특허분류

H04L 9/0852 (2013.01)

H04L 9/0819 (2013.01)

(21) 출원번호 10-2016-0174482

(22) 출원일자 2016년12월20일

심사청구일자 2016년12월20일

(71) 출원인

고려대학교 산학협력단

서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)

(72) 발명자

허준

서울특별시 강남구 광평로10길 6, 206동 103호

이성훈

서울특별시 동대문구 무학로 184, 202호

(74) 대리인

심경식, 홍성욱

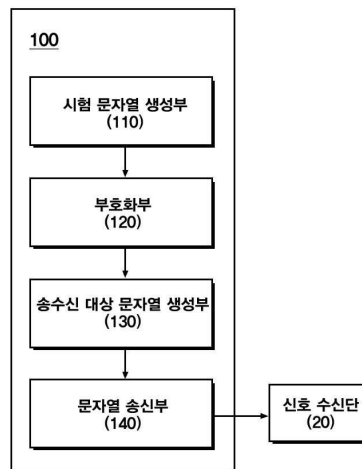
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 양자 키 분배의 정보 조정을 위한 신호 송신 장치 및 수신 장치

(57) 요약

적어도 하나의 임의의 비트값을 포함하는 문자열인 시험 문자열에 미리 저장된 생성 행렬을 곱하여 시험 문자열을 부호화한 문자열인 부호화 시험 문자열을 생성하는 부호화부, 부호화 시험 문자열 및 양자 키 분배를 통해 생성된 임의의 문자열인 신호 송신단 측 양자 키에 기초하여 송수신 대상 문자열을 생성하는 송수신 대상 문자열 생성부 및 송수신 대상 문자열을 공개 채널을 통해 신호 수신단에 전송하는 문자열 송신부를 포함하는, 양자 키 분배의 정보 조정을 위한 신호 송신 장치 및 송수신 대상 문자열을 활용하여 송신단 측 양자 키를 추정하는 양자 키 분배의 정보 조정을 위한 신호 수신 장치에 관한 것이다.

대표도 - 도1



(52) CPC특허분류

H04L 9/0858 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 1711035212

부처명 미래창조과학부

연구관리전문기관 정보통신기술진흥센터

연구사업명 정보통신기술인력양성

연구과제명 무결점 보안을 위한 지상/위성 양자통신 기술 개발

기 여 율 1/1

주관기관 고려대학교 산학협력단

연구기간 2015.06.01 ~ 2018.12.31

명세서

청구범위

청구항 1

적어도 하나의 임의의 비트값을 포함하는 문자열인 시험 문자열에 미리 저장된 생성 행렬을 곱하여 상기 시험 문자열을 부호화한 문자열인 부호화 시험 문자열을 생성하는 부호화부;

상기 부호화 시험 문자열 및 양자 키 분배를 통해 생성된 임의의 문자열인 신호 송신단 측 양자 키에 기초하여 송수신 대상 문자열을 생성하는 송수신 대상 문자열 생성부; 및

상기 송수신 대상 문자열을 공개 채널을 통해 신호 수신단에 전송하는 문자열 송신부를 포함하는, 양자 키 분배의 정보 조정을 위한 신호 송신 장치.

청구항 2

제1항에 있어서,

시험 문자열 생성부를 더 포함하며,

상기 시험 문자열 생성부는, 상기 시험 문자열을 생성하기 위한 전체 비트 중 기설정된 개수의 하위 비트에 오류 검출을 위한 순환 중복 검사 비트(CRC bit)를 각각 할당하고, 상기 전체 비트에서 상기 순환 중복 검사 비트를 제외한 나머지 비트 중 오류 정정 확률이 높은 순서대로 선택된 기설정된 개수의 비트에 상기 임의의 비트값을 각각 할당하여 상기 시험 문자열을 생성하는, 양자 키 분배의 정보 조정을 위한 신호 송신 장치.

청구항 3

제2항에 있어서,

상기 시험 문자열은,

상기 신호 송신단 측 양자 키의 비트 개수와 동일한 개수의 전체 비트 개수를 포함하는, 양자 키 분배의 정보 조정을 위한 신호 송신 장치.

청구항 4

제1항에 있어서,

상기 송수신 대상 문자열 생성부는,

상기 부호화 시험 문자열 및 상기 신호 송신단 측 양자 키를 서로 XOR 연산하여 상기 송수신 대상 문자열을 생성하는, 양자 키 분배의 정보 조정을 위한 신호 송신 장치.

청구항 5

공개 채널을 통해 송수신 대상 문자열을 신호 송신단으로부터 수신하는 문자열 수신부;

상기 송수신 대상 문자열 및 양자 키 분배를 통해 생성된 임의의 문자열인 신호 수신단 측 양자 키에 기초하여 복호 대상 문자열을 생성하는 복호 대상 문자열 생성부; 및

상기 복호 대상 문자열을 복호하여 상기 신호 송신단에서 생성한 시험 문자열을 추정한 문자열인 추정 시험 문자열을 생성하는 복호화부를 포함하는, 양자 키 분배의 정보 조정을 위한 신호 수신 장치.

청구항 6

제5항에 있어서,

상기 복호 대상 문자열 생성부는,

상기 송수신 대상 문자열 및 상기 신호 수신단 측 양자 키를 서로 XOR 연산하여 상기 복호 대상 문자열을 생성

하는, 양자 키 분배의 정보 조정을 위한 신호 수신 장치.

청구항 7

제5항에 있어서,

상기 복호화부는,

상기 복호 대상 문자열에 극 부호 복호화(Polar Code Decoding)를 적용하여 상기 추정 시험 문자열을 생성하는, 양자 키 분배의 정보 조정을 위한 신호 수신 장치.

청구항 8

제5항에 있어서,

양자 키 추정부를 더 포함하며,

상기 양자 키 추정부는, 상기 추정 시험 문자열 및 미리 저장된 생성 행렬에 기초하여 상기 신호 송신단에서 생성한 부호화 시험 문자열을 추정한 문자열인 추정 부호화 시험 문자열을 생성하고, 상기 송수신 대상 문자열 및 상기 추정 부호화 시험 문자열에 기초하여 신호 송신단 측 양자 키를 추정하는, 양자 키 분배의 정보 조정을 위한 신호 수신 장치.

청구항 9

제8항에 있어서,

상기 양자 키 추정부는,

상기 추정 시험 문자열에 상기 미리 저장된 생성 행렬을 곱하여 상기 추정 부호화 시험 문자열을 생성하는, 양자 키 분배의 정보 조정을 위한 신호 수신 장치.

청구항 10

제8항에 있어서,

상기 양자 키 추정부는,

상기 송수신 대상 문자열 및 상기 추정 부호화 시험 문자열을 서로 XOR 연산하여 상기 신호 송신단 측 양자 키를 추정하는, 양자 키 분배의 정보 조정을 위한 신호 수신 장치.

발명의 설명

기술 분야

[0001] 본 발명은 양자 키 분배(Quantum Key Distribution)의 후처리 과정인 정보 조정(Information Reconciliation)을 위한 신호 송신 장치 및 수신 장치에 관한 것이다.

배경 기술

[0002] 양자 통신은 양자들이 가지고 있는 중첩성을 이용한 통신 방법으로, 기존의 통신 방법이 주로 전자기파를 이용하여 파장 또는 진폭의 차이를 이용하여 정보를 송수신하는 방법인데 비하여, 양자 통신은 양자, 빛의 편광, 간섭 현상 등을 이용하여 정보를 송수신하는 통신 방법을 의미한다.

[0003] 이러한 양자 통신을 위하여, 신호 송신단 및 신호 수신단은 BB84 프로토콜을 활용하여 양자 채널을 통해 상호간에 암호키를 분배하게 되며, 분배된 암호키 중 신호 송신단에게 분배된 암호키를 신호 송신단 측 양자 키라 할 수 있으며, 신호 수신단에게 분배된 암호키를 신호 수신단 측 양자 키라 할 수 있고, 이러한 과정을 양자 키 분배(Quantum Key Distribution, QKD)라 한다.

[0004] 이러한, 양자 키 분배는 양자 역학의 원리에 의해 보안성이 증명되었으나, 양자 측정 기기의 불완전성, 도청자의 공격 등으로 인해 발생할 수 있는 양자 채널의 오류에 취약하며, 이러한 문제를 해결하기 위하여 양자 키 분배의 후처리 과정에는 오류가 없는 공개 채널을 통해 오류를 정정하기 위한 추가 정보를 전송하는 과정인 정보 조정(Information Reconciliation) 과정이 포함되게 된다.

[0005] 이러한, 양자 키 분배의 정보 조정 과정은 고전 통신에서의 오류 정정 부호의 적용과 유사하며, 양자 키 분배의 정보 조정 과정은 양자 키를 신호 송신단과 신호 수신단이 공유하고 난 후 양자 채널, 광자 검출 장치 등의 잡음으로 인한 오류를 정정하는 과정을 의미할 수 있다.

[0006] 예를 들어, 정보 조정 과정을 위해 제안된 캐스케이드 방식(Cascade)은 정보 조정을 위한 독자적 프로토콜로 개발되었으며, 그 성능이 뛰어남을 인정받아 사실상(de-facto) 표준으로 여겨지고 있으나, 이러한 캐스케이드 방식이 뛰어난 성능을 보이기 위해서는 신호 송신단과 신호 수신단 사이에 과도하게 많은 통신 횟수가 요구되는 단점이 있다.

선행기술문헌

특허문헌

[0007] (특허문헌 0001) 한국 등록특허공보 제10-1327661호(2013.11.04.)

발명의 내용

해결하려는 과제

[0008] 본 발명의 목적은, 상기 문제점을 해결하기 위한 것으로, 적어도 하나의 임의의 비트값을 포함하는 문자열인 시험 문자열을 활용하여 생성한 부호화 시험 문자열을 활용해 양자 키 분배의 정보 조정을 수행하도록 하여, 극 부호 부호화(Polar Code Encoding) 및 극 부호 복호화(Polar Code Decoding)를 정보 조정 과정에 적용 할 수 있도록 하기 위함이다.

[0009] 본 발명의 목적은 상기 문제점을 해결하기 위한 것으로, 시험 문자열에 오류 검출을 위한 순환 중복 검사 비트(CRC bit)를 포함하도록 하여, 양자 키 분배의 정보 조정 과정에서 극 부호 복호화(Polar Code Decoding)의 CRC 보조 리스트 복호(CRC-aided List Decoding)를 적용할 수 있도록 하기 위함이다.

[0010] 본 발명이 해결하고자 하는 과제는 이상에서 언급한 과제(들)로 제한되지 않으며, 언급되지 않은 또 다른 과제(들)는 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0011] 상기한 목적을 달성하기 위하여 본 발명의 실시예에 따른 양자 키 분배의 정보 조정을 위한 신호 송신 장치는, 적어도 하나의 임의의 비트값을 포함하는 문자열인 시험 문자열에 미리 저장된 생성 행렬을 곱하여 시험 문자열을 부호화한 문자열인 부호화 시험 문자열을 생성하는 부호화부, 부호화 시험 문자열 및 양자 키 분배를 통해 생성된 임의의 문자열인 신호 송신단 측 양자 키에 기초하여 송수신 대상 문자열을 생성하는 송수신 대상 문자열 생성부 및 송수신 대상 문자열을 공개 채널을 통해 신호 수신단에 전송하는 문자열 송신부를 포함한다.

[0012] 예컨대, 본 발명의 실시예에 따른 양자 키 분배의 정보 조정을 위한 신호 송신 장치는, 시험 문자열 생성부를 더 포함하며, 시험 문자열 생성부는, 시험 문자열을 생성하기 위한 전체 비트 중 기설정된 개수의 하위 비트에 오류 검출을 위한 순환 중복 검사 비트(CRC bit)를 각각 할당하고, 전체 비트에서 상기 순환 중복 검사 비트를 제외한 나머지 비트 중 오류 정정 확률이 높은 순서대로 선택된 기설정된 개수의 비트에 임의의 비트값을 각각 할당하여 시험 문자열을 생성한다.

[0013] 예컨대, 시험 문자열은, 신호 송신단 측 양자 키의 비트 개수와 동일한 개수의 전체 비트 개수를 포함한다.

[0014] 예컨대, 송수신 대상 문자열 생성부는, 부호화 시험 문자열 및 신호 송신단 측 양자 키를 서로 XOR 연산하여 송수신 대상 문자열을 생성한다.

[0015] 상기한 목적을 달성하기 위하여, 본 발명의 실시예에 따른, 양자 키 분배의 정보 조정을 위한 신호 수신 장치는 공개 채널을 통해 송수신 대상 문자열을 신호 송신단으로부터 수신하는 문자열 수신부, 송수신 대상 문자열 및 양자 키 분배를 통해 생성된 임의의 문자열인 신호 수신단 측 양자 키에 기초하여 복호 대상 문자열을 생성하는 복호 대상 문자열 생성부 및 복호 대상 문자열을 복호하여 신호 송신단에서 생성한 시험 문자열을 추정한 문자열인 추정 시험 문자열을 생성하는 복호화부를 포함한다.

[0016] 예컨대, 복호 대상 문자열 생성부는, 송수신 대상 문자열 및 신호 수신단 측 양자 키를 서로 XOR 연산하여 복호

대상 문자열을 생성한다.

- [0017] 일 실시예에 따라, 복호화부는, 복호 대상 문자열에 극 부호 복호화(Polar Code Decoding)를 적용하여 추정 시험 문자열을 생성한다.
- [0018] 예컨대, 본 발명의 실시예에 따른 양자 키 분배의 정보 조정을 위한 신호 수신 장치는 양자 키 추정부를 더 포함하며, 양자 키 추정부는, 추정 시험 문자열 및 미리 저장된 생성 행렬에 기초하여 신호 송신단에서 생성한 부호화 시험 문자열을 추정한 문자열인 추정 부호화 시험 문자열을 생성하고, 송수신 대상 문자열 및 추정 부호화 시험 문자열에 기초하여 신호 송신단 측 양자 키를 추정한다.
- [0019] 예를 들어, 양자 키 추정부는, 추정 시험 문자열에 미리 저장된 생성 행렬을 곱하여 추정 부호화 시험 문자열을 생성한다.
- [0020] 예컨대, 양자 키 추정부는, 송수신 대상 문자열 및 추정 부호화 시험 문자열을 서로 XOR 연산하여 신호 송신단 측 양자 키를 추정한다.

발명의 효과

- [0021] 본 발명의 일 실시예에 따르면, 양자 키 분배의 정보 조정 과정에 극 부호 부호화 및 극 부호 복호화를 적용하여, 신호 송신단과 신호 수신단 사이의 통신 횟수를 최소화하며, 신호 송신단 및 신호 수신단 사이에서 교환한 양자 키의 오류 검출을 높은 정확도로 수행할 수 있다.

도면의 간단한 설명

- [0022] 도 1은 본 발명의 실시예에 따른, 양자 키 분배의 정보 조정을 위한 신호 송신 장치를 설명하기 위한 구성도이다.
- 도 2는 본 발명의 실시예에 따른, 양자 키 분배의 정보 조정을 위한 신호 수신 장치를 설명하기 위한 구성도이다.
- 도 3은 본 발명의 실시예에 따른, 양자 키 분배의 정보 조정을 위한 신호 송신 장치의 동작 방법을 설명하기 위한 순서도이다.
- 도 4는 본 발명의 실시예에 따른, 양자 키 분배의 정보 조정을 위한 신호 수신 장치의 동작 방법을 설명하기 위한 순서도이다.
- 도 5는 본 발명의 실시예에 따른, 양자 키 분배의 정보 조정을 위한 신호 송신 장치 및 수신 장치를 설명하기 위한 도면이다.

발명을 실시하기 위한 구체적인 내용

- [0023] 이하, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 본 발명의 기술적 사상을 용이하게 실시할 수 있을 정도로 상세히 설명하기 위하여, 본 발명의 가장 바람직한 실시예를 첨부 도면을 참조하여 설명하기로 한다. 우선 각 도면의 구성요소들에 참조부호를 부가함에 있어서, 동일한 구성요소들에 대해서는 비록 다른 도면상에 표시되더라도 가능한 한 동일한 부호를 가지도록 하고 있음에 유의해야 한다. 또한, 본 발명을 설명함에 있어, 관련된 공지 구성 또는 기능에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명은 생략한다.
- [0024] 이하, 본 발명의 실시예에 따른 양자 키 분배의 정보 조정을 위한 신호 송신 장치 및 수신 장치를 첨부된 도면을 참조하여 상세하게 설명하면 아래와 같다.
- [0025] 이제 도 1 및 도 5를 동시에 참조하여, 본 발명의 실시예에 따른, 양자 키 분배의 정보 조정을 위한 신호 송신 장치를 설명한다.
- [0026] 도 1은 본 발명의 실시예에 따른, 양자 키 분배의 정보 조정을 위한 신호 송신 장치를 설명하기 위한 구성도이다.
- [0027] 도 5는 본 발명의 실시예에 따른, 양자 키 분배의 정보 조정을 위한 신호 송신 장치 및 수신 장치를 설명하기 위한 도면이다.
- [0028] 도 1에 도시된 바와 같이, 본 발명의 실시예에 따른, 양자 키 분배의 정보 조정을 위한 신호 송신 장치(100)는

부호화부(120), 송수신 대상 문자열 생성부(130) 및 문자열 송신부(140)를 포함한다.

- [0029] 예컨대, 본 발명의 실시예에 따른, 양자 키 분배의 정보 조정을 위한 신호 송신 장치(100)는 시험 문자열 생성부(110)를 더 포함할 수도 있으나, 본 발명은 이에 한정되지 않는다.
- [0030] 예컨대, 본 발명의 실시예에 따른, 양자 키 분배의 정보 조정을 위한 신호 송신 장치(100)는 도 2에 도시된 신호 송신단(10)에 포함된 일부 구성을 의미할 수 있다.
- [0031] 시험 문자열 생성부(110)는 적어도 하나의 임의의 비트값을 포함하는 문자열인 시험 문자열(v)을 생성한다.
- [0032] 예컨대, 시험 문자열(v)은 정보 조정 과정에서 극 부호 부호화 및 극 부호 복호화를 적용하기 위해 생성된 임의의 문자열을 의미할 수 있다.
- [0033] 예컨대, 시험 문자열 생성부(110)는, 시험 문자열(v)을 생성하기 위한 전체 비트 중 기설정된 개수의 하위 비트에 오류 검출을 위한 순환 중복 검사 비트(Cyclic Redundancy Check bit, CRC bit)를 각각 할당하고, 전체 비트에서 순환 중복 검사 비트를 제외한 나머지 비트 중 오류 정정 확률이 높은 순서대로 선택된 기설정된 개수의 비트에 임의의 비트값을 각각 할당하여 시험 문자열(v)을 생성한다.
- [0034] 예컨대, 시험 문자열(v)에 순환 중복 검사 비트가 포함되는 경우, 시험 문자열(v)은 정보 조정 과정에서 신호 수신단(20)이 CRC 보조 연속 제거 리스트 복호 방식을 적용하여 신호 송신단 측 양자 키를 추정하기 위해 생성된 임의의 문자열을 의미할 수 있다.
- [0035] 도 5에 도시된 바와 같이, 시험 문자열(v)이 총 8 개의 비트로 구성되고, 시험 문자열(v)에 총 1개의 순환 중복 검사 비트가 포함되며, 오류 정정 확률이 높은 순서대로 선택된 기설정된 개수의 비트가 3개인 경우를 예로 들어, 시험 문자열 생성부(110)를 설명한다.
- [0036] 이 경우, 시험 문자열 생성부(110)는 총 8개의 전체 비트(0번 비트, 1번 비트, 2번 비트, 3번 비트, 4번 비트, 5번 비트, 6번 비트 및 7번 비트) 중 1개의 하위 비트인 7번 비트에 순환 중복 검사 비트(CRC)를 할당할 수 있다.
- [0037] 그 뒤, 시험 문자열 생성부(110)는 7번 비트를 제외한 총 7개의 나머지 비트(0번 비트, 1번 비트, 2번 비트, 3번 비트, 4번 비트, 5번 비트 및 6번 비트) 중 오류 정정 확률이 가장 높은 총 3개의 비트(3번 비트, 5번 비트 및 6번 비트)에 각각 임의의 비트값(v_3 , v_5 , v_6)을 할당할 수 있다.
- [0038] 그 뒤, 시험 문자열 생성부(110)는 비트값이 할당되지 않은 총 4개의 나머지 비트(0번 비트, 1번 비트, 2번 비트 및 4번 비트)에 각각 0을 할당할 수 있다.
- [0039] 이때, 각각에 비트값 0이 할당된 비트를 고정 비트라 정의할 수 있으며, 고정 비트는 컨디션이 좋지 않은 채널로 전송되며 신호 송신단(10) 및 신호 수신단(20)이 모두 그 값을 알고 있는 비트로 신호 수신단(20)에서의 복호에 도움을 주는 비트를 의미할 수 있다.
- [0040] 상술한 과정을 거쳐서 생성된 시험 문자열(v)은 도 5에 도시된 바와 같이, (0, 0, 0, v_3 , 0, v_5 , v_6 , CRC)와 같이 나타날 수 있다.
- [0041] 예를 들어, 임의의 비트값을 할당하기 위한 기준인 오류 정정 확률이 높은 기설정된 개수의 비트는, 좋은 채널로 정보를 보내고 나쁜 채널로는 정보를 보내지 않는 채널 분극화(Channel Polarization)를 활용한 종래의 극 부호(Polar Code) 방법에서 상호 정보량이 높은 순서대로 선택된 기설정된 개수의 비트를 의미할 수 있으며, 오류 정정 확률이 높은 기설정된 개수의 비트를 선택하는 구체적인 방법은 종래의 극 부호 방법에서 제시한 방법과 동일하므로 구체적인 설명은 생략한다.
- [0042] 예컨대, 임의의 비트값을 할당하기 위한 기준인 오류 정정 확률이 높은 기설정된 개수의 비트는, 극 부호 방법에서의 고 엔트로피 집합(High-Entropy Set, E_{X^Y})을 의미할 수 있으며, 고 엔트로피 집합은 각 채널들의 조건 엔트로피(Conditional Entropy, $H(X^Y)$)가 큰 값들의 색인의 집합을 의미할 수 있다.
- [0043] 예컨대, 시험 문자열(v)은, 신호 송신단 측 양자 키(x)의 비트 개수와 동일한 개수의 전체 비트 개수를 가지도록 생성될 수 있다.
- [0044] 부호화부(120)는 적어도 하나의 임의의 비트값을 포함하는 문자열인 시험 문자열(v)에 미리 저장된 생성 행렬(G)을 곱하여 시험 문자열(v)을 부호화한 문자열인 부호화 시험 문자열(z)을 생성한다.

- [0045] 예컨대, 생성 행렬(G)은 $n \times n$ 크기의 극 부호 생성 행렬(Generator Matrix)을 의미할 수 있으며, 생성 행렬(G)은 역행렬이 자기 자신인 각종 행렬을 의미할 수 있다.
- [0046] 예컨대, 생성 행렬(G)은 극 부호 부호화(Polar Code Encoding)에서 오류 정정 부호를 생성하기 위해 활용되는 행렬 형태로 표시되는 변환 연산자로 비트-반전(Bit-Reversal) 행렬을 비롯한 각종 행렬을 의미할 수 있으며, 본 발명은 극 부호 생성 행렬의 종류에 한정되지 않는다.
- [0047] 예컨대, 부호화부(120)는 폴라 코드 인코더(Polar Code Encoder)를 의미할 수 있으나, 본 발명은 이에 한정되지 않는다.
- [0048] 예를 들어, 도 5에 도시된 바와 같이, 시험 문자열(v)과 생성 행렬(G)을 곱하면 부호화 시험 문자열(z)이 생성 ($z = vG$)될 수 있으며, 부호화부(120)가 시험 문자열(v)을 부호화 하는 방법은 극 부호 부호화(Polar Code Encoding)를 의미할 수 있고, 이는 일종의 가상 부호화를 의미할 수 있다.
- [0049] 상술한 시험 문자열 생성부(110) 및 부호화부(120)를 통해, 본 발명의 실시예에 따른, 양자 키 분배의 정보 조정을 위한 신호 송신 장치(100)는 양자 키 분배의 후처리 과정 중 하나인 정보 조정 과정에서 극 부호 부호화가 적용될 수 있도록 할 수 있다.
- [0050] 특히, 시험 문자열(v)에 순환 중복 검사 비트가 포함되는 경우, 본 발명의 실시예에 따른, 양자 키 분배의 정보 조정을 위한 신호 송신 장치(100)는 신호 수신단(20)이 극 부호 복호화의 CRC 보조 연속 제거 리스트 복호를 수행할 수 있도록 하여, 정보 조정의 성능을 향상시킬 수 있다.
- [0051] 예를 들어, 신호 송신단 측 양자 키(x)를 공개 채널로 신호 수신단(20)에 직접 전송하여 신호 수신단 측 양자 키(y)와 비교하는 종래의 정보 조정 과정에서는 신호 송신단 측 양자 키(x)가 양자 키 분배를 통해 생성된 임의의 문자열이기 때문에, 순환 중복 검사 비트를 부가할 수 없으며 이 때문에 정보 조정 과정에서 극 부호 복호화의 CRC 보조 연속 제거 리스트 복호를 수행할 수 없는 문제가 있으나, 본 발명의 실시예에 따른, 양자 키 분배의 정보 조정을 위한 신호 송신 장치(100)는 별도의 시험 문자열(v)을 활용하기 때문에 순환 중복 검사 비트를 활용할 수 있는 효과가 있다.
- [0052] 송수신 대상 문자열 생성부(130)는 부호화 시험 문자열(z) 및 양자 키 분배를 통해 생성된 임의의 문자열인 신호 송신단 측 양자 키(x)에 기초하여 송수신 대상 문자열(u)을 생성한다.
- [0053] 예컨대, 신호 송신단 측 양자 키(x)는 양자 키 분배를 통해 신호 송신단(10)에 할당된 양자 키를 의미할 수 있다.
- [0054] 예컨대, 신호 송신단 측 양자 키(x)는 BB84 프로토콜에 기초하여, 광자의 전송 및 측정을 통해 생성된 임의의 문자열을 의미할 수 있으나, 본 발명은 이에 한정되지 않는다.
- [0055] 예를 들어, 도 5에 도시된 바와 같이, 송수신 대상 문자열 생성부(130)는 부호화 시험 문자열(z) 및 신호 송신단 측 양자 키(x)를 서로 XOR 연산하여 송수신 대상 문자열(u)을 생성($u = z \oplus x$)할 수 있다.
- [0056] 문자열 송신부(140)는 송수신 대상 문자열(u)을 공개 채널을 통해 신호 수신단(20)에 전송한다.
- [0057] 이제 도 2 및 도 5를 동시에 참조하여, 본 발명의 실시예에 따른, 양자 키 분배의 정보 조정을 위한 신호 수신 장치를 설명한다.
- [0058] 도 2는 본 발명의 실시예에 따른, 양자 키 분배의 정보 조정을 위한 신호 수신 장치를 설명하기 위한 구성도이다.
- [0059] 도 5는 본 발명의 실시예에 따른, 양자 키 분배의 정보 조정을 위한 신호 송신 장치 및 수신 장치를 설명하기 위한 도면이다.
- [0060] 도 2에 도시된 바와 같이, 본 발명의 실시예에 따른, 양자 키 분배의 정보 조정을 위한 신호 수신 장치(200)는 문자열 수신부(210), 복호 대상 문자열 생성부(220) 및 복호화부(230)를 포함한다.
- [0061] 예컨대, 본 발명의 실시예에 따른, 양자 키 분배의 정보 조정을 위한 신호 수신 장치(200)는 양자 키 추정부(240)를 더 포함할 수 있으나, 본 발명은 이에 한정되지 않는다.
- [0062] 예컨대, 본 발명의 실시예에 따른, 양자 키 분배의 정보 조정을 위한 신호 수신 장치(200)는 도 1에 도시된 신

호 수신단(20)에 포함된 일부 구성을 의미할 수 있다.

[0063] 문자열 수신부(210)는 공개 채널을 통해 송수신 대상 문자열(u)을 신호 송신단(10)으로부터 수신한다.

[0064] 복호 대상 문자열 생성부(220)는 송수신 대상 문자열(u) 및 양자 키 분배를 통해 생성된 임의의 문자열인 신호 수신단 측 양자 키(y)에 기초하여 복호 대상 문자열(w)을 생성한다.

[0065] 예컨대, 신호 수신단 측 양자 키(y)는 양자 키 분배를 통해 신호 수신단(20)에 할당된 양자 키를 의미할 수 있다.

[0066] 예컨대, 신호 수신단 측 양자 키(y)는 BB84 프로토콜에 기초하여, 광자의 전송 및 측정을 통해 생성된 임의의 문자열을 의미할 수 있으나, 본 발명은 이에 한정되지 않는다.

[0067] 예를 들어, 도 5에 도시된 바와 같이, 복호 대상 문자열 생성부(220)는, 송수신 대상 문자열(u) 및 신호 수신단 측 양자 키(y)를 서로 XOR 연산하여 복호 대상 문자열(w)을 생성($w = u \oplus y$)할 수 있다.

[0068] 이제, 하기의 수학식 1 내지 6을 통해, 본 발명의 실시예에 따른, 양자 키 분배의 정보 조정을 위한 신호 송신 장치 및 수신 장치에서 부호화 시험 문자열(z)이 신호 송신단 측 양자 키(x)의 역할을 대체하고, 복호 대상 문자열(w)이 신호 수신단 측 양자 키(y)의 역할을 대체할 수 있음을 설명한다.

[0069] 종래의 양자 키 분배의 정보 조정 과정에서 신호 송신단 측 양자 키(x) 및 신호 수신단 측 양자 키(y)의 관계 아래 수학식 1의 관계식으로 설명될 수 있다.

[0070] [수학식 1]

[0071]
$$y = x \oplus e$$

[0072] 이때, y는 신호 수신단 측 양자 키, x는 신호 송신단 측 양자 키 e는 에러 벡터를 의미한다.

[0073] 한편, 일 실시예에 따른 복호 대상 문자열(w)은 상술한 바와 같이 아래 수학식 2 와 같이 표현될 수 있다.

[0074] [수학식 2]

[0075]
$$w = u \oplus y$$

[0076] 이때, w는 복호 대상 문자열, u는 송수신 대상 문자열, y는 신호 수신단 측 양자 키를 의미한다.

[0077] 한편, 본 발명의 실시예에 따른, 양자 키 분배의 정보 조정을 위한 신호 송신 장치(100)가 생성한 송수신 대상 문자열(u)은 상술한 바와 같이 아래 수학식 3을 만족한다.

[0078] [수학식 3]

[0079]
$$u = z \oplus x$$

[0080] 이때, u는 송수신 대상 문자열, z는 부호화 시험 문자열, x는 신호 송신단 측 양자 키를 의미한다.

[0081] 여기서, 수학식 3을 수학식 4에 대입하면 아래와 같은 수학식 5가 유도될 수 있다.

[0082] [수학식 5]

[0083]
$$w = z \oplus x \oplus y$$

[0084] 이때, w는 복호 대상 문자열, z는 부호화 시험 문자열, x는 신호 송신단 측 양자 키, y는 신호 수신단 측 양자 키를 의미한다.

[0085] 여기서, 수학식 5에 상술한 수학식 1을 대입하면, XOR 연산의 성질에 기초하여 아래 수학식 6이 유도될 수 있다.

[0086] [수학식 6]

$$w = z \oplus e$$

[0087]

[0088] 이때, w 는 복호 대상 문자열, z 는 부호화 시험 문자열, e 는 에러 벡터를 의미한다.

[0089] 그 결과, 수학식 1과 수학식 6을 비교하면, 부호화 시험 문자열(z)이 신호 송신단 측 양자 키(x)의 역할을 대체하고, 복호 대상 문자열(w)이 신호 수신단 측 양자 키(y)의 역할을 대체할 수 있음을 확인할 수 있다.

[0090] 다시 말해, 본 발명의 실시예에 따른, 양자 키 분배의 정보 조정을 위한 신호 송신 장치 및 수신 장치에서 시험 문자열(v) 및 순환 중복 검사 비트(CRC bit)를 활용한 극 부호 부호화 및 극 부호 복호화를 적용하더라도, 부호화 시험 문자열(z) 및 복호 대상 문자열(w)에 기초하여 양자 키 분배의 정보 조정이 수행될 수 있음을 확인할 수 있다.

[0091] 복호화부(230)는 복호 대상 문자열(w)을 복호하여 신호 송신단(10)에서 생성한 시험 문자열(v)을 추정한 문자열인 추정 시험 문자열($\hat{v}$)을 생성한다.

[0092] 예컨대, 복호화부(230)는, 복호 대상 문자열(w)에 극 부호 복호화(Polar Code Decoding)를 적용하여 추정 시험 문자열($\hat{v}$)을 생성한다.

[0093] 예컨대, 복호화부(230)는 시험 문자열(v)에 비트값 0이 할당된 비트인 고정 비트에 대한 정보를 활용하여 복호화를 수행하여 추정 시험 문자열($\hat{v}$)을 생성할 수도 있다.

[0094] 예를 들어, 신호 송신단(10)에서 생성한 시험 문자열(v)이 순환 중복 검사 비트(CRC bit)를 포함하지 않는 경우, 복호화부(230)는 극 부호 복호화(Polar Code Decoding)의 일종인 연속 제거 복호 방식을 활용하여 복호 대상 문자열(w)을 복호함으로써 추정 시험 문자열($\hat{v}$)을 생성할 수 있다.

[0095] 예컨대, 신호 송신단(10)에서 생성한 시험 문자열(v)이 순환 중복 검사 비트(CRC bit)를 포함하는 경우, 복호화부(230)는 극 부호 복호화(Polar Code Decoding)의 일종인 CRC 보조 연속 제거 리스트 복호를 활용하여 복호 대상 문자열(w)을 복호함으로써 추정 시험 문자열($\hat{v}$)을 생성할 수 있다.

[0096] 이때, 극 부호 복호화의 일종인, 연속 제거 복호 방식 및 CRC 보조 연속 제거 리스트 복호에 대한 구체적인 설명은 종래에 고전 통신 방법에서 공지된 바와 같으므로, 구체적인 설명은 생략한다.

[0097] 예컨대, 복호화부(230)는 폴라 코드 디코더(Polar Code Decoder)를 의미할 수 있으나, 본 발명은 이에 한정되지 않는다.

[0098] 예컨대, 복호 대상 문자열(w)을 복호하여 생성된 추정 시험 문자열($\hat{v}$)은 도 5에 도시된 바와 같이 나타날 수 있다.

[0099] 예컨대, 양자 키 추정부(240)는, 추정 시험 문자열($\hat{v}$) 및 미리 저장된 생성 행렬(G)에 기초하여 신호 송신단(10)에서 생성한 부호화 시험 문자열(z)을 추정한 문자열인 추정 부호화 시험 문자열($\hat{z}$)을 생성하고, 송수신 대상 문자열(u) 및 추정 부호화 시험 문자열($\hat{z}$)에 기초하여 신호 송신단 측 양자 키(x)를 추정할 수 있다.

[0100] 보다 상세하게, 양자 키 추정부(240)는, 추정 시험 문자열($\hat{v}$)에 미리 저장된 생성 행렬(G)을 곱하여 추정 부호화 시험 문자열($\hat{z}$)을 생성($\hat{z} = \hat{v}G$)할 수 있다.

[0101] 나아가, 양자 키 추정부(240)는, 송수신 대상 문자열(u) 및 추정 부호화 시험 문자열($\hat{z}$)을 서로 XOR 연산하여 신호 송신단 측 양자 키(x)를 추정할 수 있다.

[0102] 예를 들어, 상술한 수학식 3에 XOR 연산의 성질을 적용하면, 아래 수학식 7이 유도될 수 있으며, 양자 키 추정

부(240)는 아래 수식 7에 기초하여 신호 송신단 측 양자 키(x)를 추정할 수 있다.

[수식 7]

$$\hat{x} = u \oplus \hat{z}$$

이때, $\hat{x}$ 는 신호 송신단 측 양자 키(x)를 추정 결과, u는 송수신 대상 문자열, $\hat{z}$ 추정 부호화 시험 문자열을 의미한다.

이제 도 3을 참조하여, 본 발명의 실시예에 따른, 양자 키 분배의 정보 조정을 위한 신호 송신 장치(100)의 동작 방법을 설명한다.

도 3은 본 발명의 실시예에 따른, 양자 키 분배의 정보 조정을 위한 신호 송신 장치의 동작 방법을 설명하기 위한 순서도이다.

S310 단계에서, 시험 문자열 생성부(110)는 적어도 하나의 임의의 비트값을 포함하는 문자열인 시험 문자열(v)을 생성한다.

S330 단계에서 부호화부(120)는 적어도 하나의 임의의 비트값을 포함하는 문자열인 시험 문자열(v)에 미리 저장된 생성 행렬(G)을 곱하여 시험 문자열(v)을 부호화한 문자열인 부호화 시험 문자열(z)을 생성한다.

S350 단계에서, 송수신 대상 문자열 생성부(130)는 부호화 시험 문자열(z) 및 양자 키 분배를 통해 생성된 임의의 문자열인 신호 송신단 측 양자 키(x)에 기초하여 송수신 대상 문자열(u)을 생성한다.

S370 단계에서, 문자열 송신부(140)는 송수신 대상 문자열(u)을 공개 채널을 통해 신호 수신단(20)에 전송한다.

이제 도 4를 참조하여, 본 발명의 실시예에 따른, 양자 키 분배의 정보 조정을 위한 신호 수신 장치(200)의 동작 방법을 설명한다.

도 4은 본 발명의 실시예에 따른, 양자 키 분배의 정보 조정을 위한 신호 수신 장치의 동작 방법을 설명하기 위한 순서도이다.

S410 단계에서, 문자열 수신부(210)는 공개 채널을 통해 송수신 대상 문자열(u)을 신호 송신단(10)으로부터 수신한다.

S430 단계에서, 복호 대상 문자열 생성부(220)는 송수신 대상 문자열(u) 및 양자 키 분배를 통해 생성된 임의의 문자열인 신호 수신단 측 양자 키(y)에 기초하여 복호 대상 문자열(w)을 생성한다.

S450 단계에서, 복호화부(230)는 복호 대상 문자열(w)을 복호하여 신호 송신단(10)에서 생성한 시험 문자열(v)을 추정한 문자열인 추정 시험 문자열($\hat{v}$)을 생성한다.

S470 단계에서, 양자 키 추정부(240)는 추정 시험 문자열($\hat{v}$) 및 미리 저장된 생성 행렬(G)에 기초하여 신호 송신단(10)에서 생성한 부호화 시험 문자열(z)을 추정한 문자열인 추정 부호화 시험 문자열($\hat{z}$)을 생성하고, 송수신 대상 문자열(u) 및 추정 부호화 시험 문자열($\hat{z}$)에 기초하여 신호 송신단(10) 측 양자 키(x)를 추정한다.

이상에서 본 발명에 따른 바람직한 실시예에 대해 설명하였으나, 다양한 형태로 변형이 가능하며, 본 기술분야에서 통상의 지식을 가진 자라면 본 발명의 특허청구범위를 벗어남이 없이 다양한 변형예 및 수정예를 실시할 수 있을 것으로 이해된다.

부호의 설명

10: 신호 송신단 20: 신호 수신단

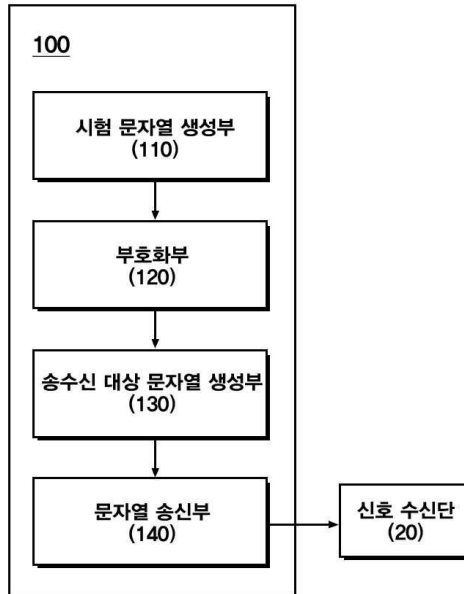
100: 양자 키 분배의 정보 조정을 위한 신호 송신 장치

110: 시험 문자열 생성부 120: 부호화부

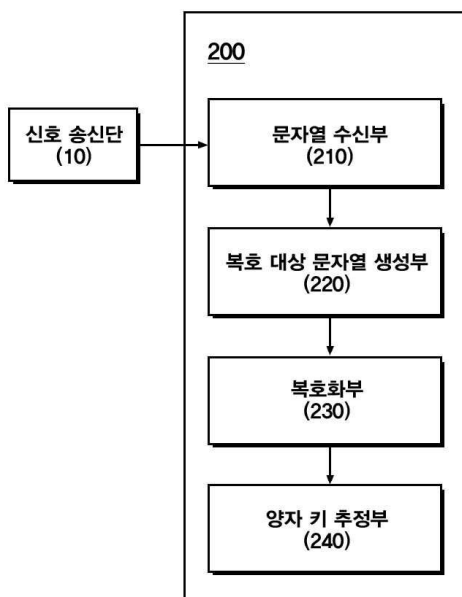
130: 송수신 대상 문자열 생성부 140: 문자열 송신부
 200: 양자 키 분배의 정보 조정을 위한 신호 수신 장치
 210: 문자열 수신부 220: 복호 대상 문자열 생성부
 230: 복호화부 240: 양자 키 추정부

도면

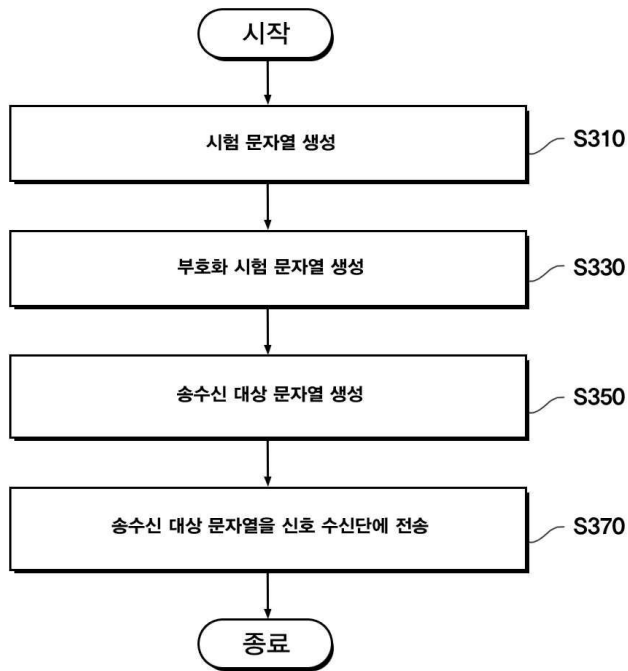
도면1



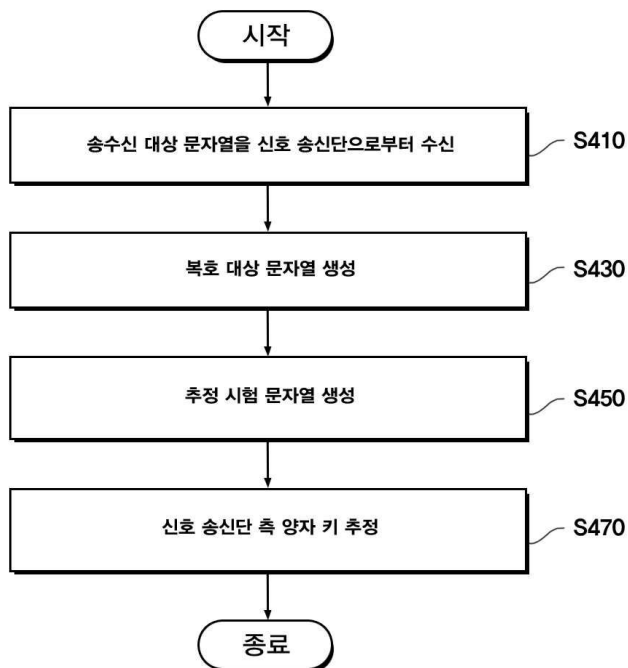
도면2



도면3



도면4



도면5

