(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2019-0001165
(43) 공개일자 2019년01월04일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *H04L 1/00* (2006.01)
H04L 1/24 (2006.01)
(52) CPC특허분류
H04L 9/0858 (2013.01)
H04L 1/0016 (2013.01)
(21) 출원번호 10-2017-0080716
(22) 출원일자 2017년06월26일
심사청구일자 2017년06월26일

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
허준
서울특별시 강남구 광평로10길 6, 206동 103호
신정환
서울특별시 강서구 마곡중앙1로 72, 1016동 1404호
임문수
경기도 고양시 덕양구 토당로 93, 101동 1006호
(74) 대리인
심경식, 홍성욱

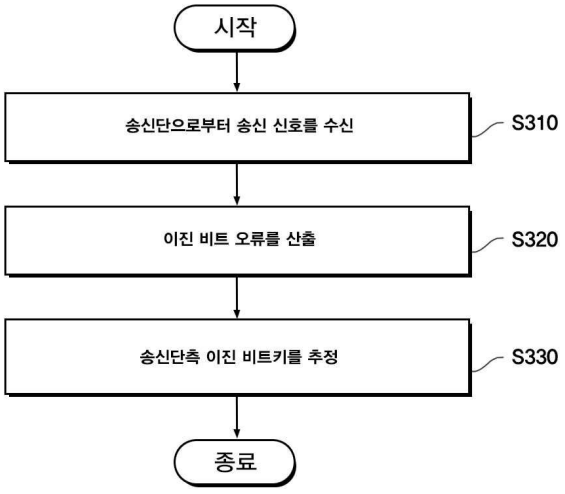
전체 청구항 수 : 총 8 항

(54) 발명의 명칭 **연속 변수 양자키 분배의 정보 조정을 위한 이진 비트키 추정 방법 및 장치**

(57) 요 약

정보 수신부가, 송신단측 이진 비트키에 기초하여 생성된 송신 신호를 송신단으로부터 수신하는 단계, 오류 산출부가, 송신 신호, 미리 저장된 수신단측 이진 비트키 및 기설정된 패리티 체크 행렬(Parity Check Matrix) 중 적어도 하나에 기초하여 송신단측 이진 비트키와 수신단측 이진 비트키 상호 간의 차이를 나타내는 이진 비트 오류를 산출하는 단계 및 이진 비트키 추정부가, 수신단측 이진 비트키 및 이진 비트 오류에 기초하여 송신단측 이진 비트키를 추정하는 단계를 포함하는, 연속 변수 양자키 분배의 정보 조정을 위한 이진 비트키 추정 방법 및 이를 위한 장치에 관한 것이다.

대 표 도 - 도3



(52) CPC특허분류
H04L 1/246 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711042435
부처명 미래창조과학부
연구관리전문기관 정보통신기술진흥센터
연구사업명 IT·SW융합산업원천기술개발
연구과제명 양자암호통신망 구축을 통한 신뢰성 검증기술 및 QKD 고도화를 위한 핵심요소기술 개발
기 여 율 1/1
주관기관 고려대학교 산학협력단
연구기간 2016.06.01 ~ 2017.05.31

명 세 서

청구범위

청구항 1

정보 수신부가, 송신단측 이진 비트키에 기초하여 생성된 송신 신호를 송신단으로부터 수신하는 단계;

오류 산출부가, 상기 송신 신호, 미리 저장된 수신단측 이진 비트키 및 기설정된 패리티 체크 행렬(Parity Check Matrix) 중 적어도 하나에 기초하여 상기 송신단측 이진 비트키와 상기 수신단측 이진 비트키 상호 간의 차이를 나타내는 이진 비트 오류를 산출하는 단계; 및

이진 비트키 추정부가, 상기 수신단측 이진 비트키 및 상기 이진 비트 오류에 기초하여 상기 송신단측 이진 비트키를 추정하는 단계를 포함하는, 연속 변수 양자키 분배의 정보 조정을 위한 이진 비트키 추정 방법.

청구항 2

제1항에 있어서,

상기 송신 신호는,

상기 송신단측 이진 비트키 및 미리 선택된 임의의 부호어(Codeword)를 XOR 연산하여 생성된 신호인, 연속 변수 양자키 분배의 정보 조정을 위한 이진 비트키 추정 방법.

청구항 3

제1항에 있어서,

상기 이진 비트 오류를 산출하는 단계는,

상기 송신 신호 및 상기 미리 저장된 수신단측 이진 비트키를 XOR 연산하여 제1 연산값을 생성하는 단계;

상기 기설정된 패리티 체크 행렬에 상기 제1 연산값을 행렬곱 연산하여 제2 연산값을 생성하는 단계; 및

미리 저장된 룩업 테이블(Lookup Table)에 기초하여 상기 제2 연산값에 대응되는 상기 이진 비트 오류를 결정하는 단계를 포함하는, 연속 변수 양자키 분배의 정보 조정을 위한 이진 비트키 추정 방법.

청구항 4

제1항에 있어서,

상기 송신단측 이진 비트키를 추정하는 단계는,

상기 수신단측 이진 비트키 및 상기 이진 비트 오류를 XOR 연산하여 상기 송신단측 이진 비트키를 추정하는 단계를 포함하는, 연속 변수 양자키 분배의 정보 조정을 위한 이진 비트키 추정 방법.

청구항 5

송신단측 이진 비트키에 기초하여 생성된 송신 신호를 송신단으로부터 수신하는 정보 수신부;

상기 송신 신호, 미리 저장된 수신단측 이진 비트키 및 기설정된 패리티 체크 행렬(Parity Check Matrix) 중 적어도 하나에 기초하여 상기 송신단측 이진 비트키와 상기 수신단측 이진 비트키 상호 간의 차이를 나타내는 이진 비트 오류를 산출하는 오류 산출부; 및

상기 수신단측 이진 비트키 및 상기 이진 비트 오류에 기초하여 상기 송신단측 이진 비트키를 추정하는 이진 비트키 추정부를 포함하는, 연속 변수 양자키 분배의 정보 조정을 위한 이진 비트키 추정 장치.

청구항 6

제5항에 있어서,

상기 송신 신호는,

상기 송신단측 이진 비트키 및 미리 선택된 임의의 부호어(Codeword)를 XOR 연산하여 생성된 신호인, 연속 변수 양자키 분배의 정보 조정을 위한 이진 비트키 추정 장치.

청구항 7

제5항에 있어서,

상기 오류 산출부는,

상기 송신 신호 및 상기 미리 저장된 수신단측 이진 비트키를 XOR 연산하여 제1 연산값을 생성하고,

상기 기설정된 패리티 체크 행렬에 상기 제1 연산값을 행렬곱 연산하여 제2 연산값을 생성하고,

미리 저장된 룩업 테이블(Lookup Table)에 기초하여 상기 제2 연산값에 대응되는 상기 이진 비트 오류를 결정하는, 연속 변수 양자키 분배의 정보 조정을 위한 이진 비트키 추정 장치.

청구항 8

제5항에 있어서,

상기 이진 비트키 추정부는,

상기 수신단측 이진 비트키 및 상기 이진 비트 오류를 XOR 연산하여 상기 송신단측 이진 비트키를 추정하는, 연속 변수 양자키 분배의 정보 조정을 위한 이진 비트키 추정 장치.

발명의 설명

기 술 분 야

[0001] 본 발명은 연속 변수 양자 키 분배(Continuous Variable Quantum Key Distribution)의 후처리 과정인 정보 조정(Information Reconciliation)을 위한 이진 비트키 추정 방법 및 장치에 관한 것이다.

배 경 기 술

[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, 송신단(Alice) 및 수신단(Bob)은 양자 채널을 통해 상호 간에 암호키를 분배하게 되며, 분배된 암호키 중 송신단(Alice)에게 분배된 암호키를 송신단측 양자키라 할 수 있으며, 수신단(Bob)에게 분배된 암호키를 수신단측 양자키라 할 수 있고, 이러한 과정을 양자키 분배(Quantum Key Distribution, QKD)라 한다.

[0004] 이때, 송신단측 양자키 및 수신단측 양자키 모두가 연속 변수로 이루어진 경우 상술한 과정은 연속 변수 양자키 분배(Continuous Variable Quantum Key Distribution, CV-QKD)라 한다.

[0005] 여기서, 연속 변수 양자키 분배(Continuous Variable Quantum Key Distribution, CV-QKD)에서 송신단 및 수신단 각각은 자신의 양자키를 서로 동일한 규칙으로 양자화(Quantization)하여 이진 비트키를 생성하며, 이때 송신단이 보유한 이진 비트키를 송신단측 이진 비트키라하고, 수신단이 보유한 이진 비트키를 수신단측 이진 비트키라 할 수 있다.

[0006] 이때, 양자 채널(Quantum Channel)의 특성 및 이진 비트키 생성의 랜덤성 때문에 송신단측 이진 비트키와 수신단측 이진 비트키는 서로 달라지게 되며, 그 결과 송신단측 이진 비트키와 수신단측 이진 비트키를 서로 동일하게 하는 과정이 필요하며 이를 정보 조정(Information Reconciliation) 과정이라 한다.

[0007] 이러한, 연속 변수 양자키 분배(CV-QKD)의 후처리 과정인 정보 조정(Information Reconciliation)을 위하여 종래에는 슬라이스드 리컨실리에이션(Sliced Reconciliation) 방법이 활용되었다.

[0008] 슬라이스드 리컨실리에이션(Sliced Reconciliation) 방법은 송신단측 이진 비트키와 수신단측 이진 비트키 각각을 병렬로 나열한 후, 이 중 도청자가 이미 알고 있을 확률이 높은 이진 비트키의 비트들을 인코딩하여 고전 채널을 통해 공유함으로써 전체를 정정하고, 이러한 과정에서 도청자가 알아냈을 가능성이 높은 비트들을 버리고

남은 키를 공유하는 과정으로 진행된다.

[0009] 그러나, 이러한 슬라이스드 리컨실리에이션(Sliced Reconciliation) 방법은 복잡도가 매우 높으며, 플로팅(Floating) 값을 저장해야 하기 때문에 메모리의 필요량이 많은 문제가 있다.

선행기술문헌

특허문헌

[0010] (특허문헌 0001) 한국 공개특허공보 제10-2015-0031245호(2015.03.23.)

발명의 내용

해결하려는 과제

[0011] 본 발명의 목적은, 상기 문제점을 해결하기 위한 것으로, 송신단측 이진 비트키에 기초하여 생성된 송신 신호를 송신단으로부터 수신하고, 송신 신호, 미리 저장된 수신단측 이진 비트키 및 기설정된 패리티 체크 행렬(Parity Check Matrix) 중 적어도 하나에 기초하여 송신단측 이진 비트키와 수신단측 이진 비트키 상호 간의 차이를 나타내는 이진 비트 오류를 산출한 뒤, 수신단측 이진 비트키 및 이진 비트 오류에 기초하여 송신단측 이진 비트키를 추정하기 위함이다.

[0012] 본 발명이 해결하고자 하는 과제는 이상에서 언급한 과제(들)로 제한되지 않으며, 언급되지 않은 또 다른 과제(들)은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0013] 상기한 목적을 달성하기 위하여 본 발명의 실시예에 따른 연속 변수 양자키 분배의 정보 조정을 위한 이진 비트키 추정 방법은 정보 수신부가, 송신단측 이진 비트키에 기초하여 생성된 송신 신호를 송신단으로부터 수신하는 단계, 오류 산출부가, 송신 신호, 미리 저장된 수신단측 이진 비트키 및 기설정된 패리티 체크 행렬(Parity Check Matrix) 중 적어도 하나에 기초하여 송신단측 이진 비트키와 수신단측 이진 비트키 상호 간의 차이를 나타내는 이진 비트 오류를 산출하는 단계 및 이진 비트키 추정부가, 수신단측 이진 비트키 및 이진 비트 오류에 기초하여 송신단측 이진 비트키를 추정하는 단계를 포함한다.

[0014] 예컨대, 송신 신호는, 송신단측 이진 비트키 및 미리 선택된 임의의 부호어(Codeword)를 XOR 연산하여 생성된 신호이다.

[0015] 일 실시예에 따라, 이진 비트 오류를 산출하는 단계는, 송신 신호 및 미리 저장된 수신단측 이진 비트키를 XOR 연산하여 제1 연산값을 생성하는 단계, 기설정된 패리티 체크 행렬에 제1 연산값을 행렬곱 연산하여 제2 연산값을 생성하는 단계 및 미리 저장된 룩업 테이블(Lookup Table)에 기초하여 제2 연산값에 대응되는 이진 비트 오류를 결정하는 단계를 포함한다.

[0016] 예컨대, 송신단측 이진 비트키를 추정하는 단계는, 수신단측 이진 비트키 및 이진 비트 오류를 XOR 연산하여 송신단측 이진 비트키를 추정하는 단계를 포함한다.

[0017] 상기한 목적을 달성하기 위하여, 본 발명의 실시예에 따른 연속 변수 양자키 분배의 정보 조정을 위한 이진 비트키 추정 장치는 송신단측 이진 비트키에 기초하여 생성된 송신 신호를 송신단으로부터 수신하는 정보 수신부, 송신 신호, 미리 저장된 수신단측 이진 비트키 및 기설정된 패리티 체크 행렬(Parity Check Matrix) 중 적어도 하나에 기초하여 송신단측 이진 비트키와 수신단측 이진 비트키 상호 간의 차이를 나타내는 이진 비트 오류를 산출하는 오류 산출부 및 수신단측 이진 비트키 및 이진 비트 오류에 기초하여 송신단측 이진 비트키를 추정하는 이진 비트키 추정부를 포함한다.

[0018] 예컨대, 송신 신호는, 송신단측 이진 비트키 및 미리 선택된 임의의 부호어(Codeword)를 XOR 연산하여 생성된 신호이다.

[0019] 예컨대, 오류 산출부는, 송신 신호 및 미리 저장된 수신단측 이진 비트키를 XOR 연산하여 제1 연산값을 생성하고, 기설정된 패리티 체크 행렬에 제1 연산값을 행렬곱 연산하여 제2 연산값을 생성하고, 미리 저장된 룩업 테이블(Lookup Table)에 기초하여 제2 연산값에 대응되는 이진 비트 오류를 결정한다.

[0020] 일 실시예에 따라, 이진 비트키 추정부는, 수신단측 이진 비트키 및 이진 비트 오류를 XOR 연산하여 송신단측 이진 비트키를 추정한다.

발명의 효과

[0021] 본 발명의 일 실시예에 따르면, 송신단측 이진 비트키에 기초하여 생성된 송신 신호를 송신단으로부터 수신하고, 송신 신호, 미리 저장된 수신단측 이진 비트키 및 기설정된 패리티 체크 행렬(Parity Check Matrix) 중 적어도 하나에 기초하여 송신단측 이진 비트키와 수신단측 이진 비트키 상호 간의 차이를 나타내는 이진 비트 오류를 산출한 뒤, 수신단측 이진 비트키 및 이진 비트 오류에 기초하여 송신단측 이진 비트키를 추정함으로써, 정보 조정(Information Reconciliation) 과정을 통한 오류 정정을 간소화할 수 있는 효과가 있다.

도면의 간단한 설명

[0022] 도 1은 본 발명의 실시예에 따른, 연속 변수 양자키 분배의 정보 조정을 위한 이진 비트키 추정 장치가 적용되는 송신단(Alice) 및 수신단(Bob)의 관계를 설명하기 위한 도면이다.

도 2는 본 발명의 실시예에 따른, 연속 변수 양자키 분배의 정보 조정을 위한 이진 비트키 추정 장치를 설명하기 위한 구성도이다.

도 3은 본 발명의 실시예에 따른, 연속 변수 양자키 분배의 정보 조정을 위한 이진 비트키 추정 방법을 설명하기 위한 순서도이다.

도 4는 본 발명의 실시예에 따른, 연속 변수 양자키 분배의 정보 조정을 위한 이진 비트키 추정 방법에서 이진 비트 오류를 산출하는 단계를 설명하기 위한 순서도이다.

도 5는 본 발명의 실시예에 따른, 연속 변수 양자키 분배의 정보 조정을 위한 이진 비트키 추정 방법 및 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 연속 변수 양자키 분배의 정보 조정을 위한 이진 비트키 추정 방법 및 장치를 첨부된 도면을 참조하여 상세하게 설명하면 아래와 같다.

[0025] 우선 도 1 및 도 5를 동시에 참조하여, 본 발명의 실시예에 따른 연속 변수 양자키 분배의 정보 조정을 위한 이진 비트키 추정 장치(200)가 적용되는 수신단(20, Bob) 및 송신단(10, Alice)의 관계를 설명한다.

[0026] 도 1은 본 발명의 실시예에 따른, 연속 변수 양자키 분배의 정보 조정을 위한 이진 비트키 추정 장치가 적용되는 송신단(Alice) 및 수신단(Bob)의 관계를 설명하기 위한 도면이다.

[0027] 도 5는 본 발명의 실시예에 따른, 연속 변수 양자키 분배의 정보 조정을 위한 이진 비트키 추정 방법 및 장치를 설명하기 위한 도면이다.

[0028] 도 1에 도시된 바와 같이, 연속 변수 양자키 분배(CV-QKD)에서는 정보를 송신하는 송신단(10, Alice) 및 정보를 수신하는 수신단(20, Bob)이 포함되며, 이들 송신단(10, Alice) 및 수신단(20, Bob)는 연속 변수 양자키 분배(CV-QKD)를 통해 양자 통신을 위해 서로 공유하는 암호키를 분배하게 된다.

[0029] 이때, 본 발명의 실시예에 따른 연속 변수 양자키 분배의 정보 조정을 위한 이진 비트키 추정 장치(200)는 도 1에 도시된 송신단(10, Alice) 또는 수신단(20, Bob) 중 어느 하나에 포함되어, 상대방의 이진 비트키를 추정한다.

[0030] 즉, 본 발명의 실시예에 따른 연속 변수 양자키 분배의 정보 조정을 위한 이진 비트키 추정 장치(200)가 송신단(10, Alice)에 포함된 경우, 연속 변수 양자키 분배의 정보 조정을 위한 이진 비트키 추정 장치(200)는 수신단

(20, Bob)이 보유한 이진 비트키인 수신단측 이진 비트키를 추정할 수 있다.

[0031] 반대로, 본 발명의 실시예에 따른 연속 변수 양자키 분배의 정보 조정을 위한 이진 비트키 추정 장치(200)가 수신단(20, Bob)에 포함된 경우, 연속 변수 양자키 분배의 정보 조정을 위한 이진 비트키 추정 장치(200)는 송신단(10, Alice)이 보유한 이진 비트키인 송신단측 이진 비트키를 추정할 수 있다.

[0032] 이를 통해, 송신단(10, Alice) 및 수신단(20, Bob)은 서로 동일한 암호키인 이진 비트키를 공유할 수 있게 되며, 서로 공유된 이진 비트키를 통해 양자 통신을 수행할 수 있게 된다.

[0033] 계속, 도 5를 참조하여, 본 발명의 실시예에 따른 연속 변수 양자키 분배의 정보 조정을 위한 이진 비트키 추정 방법 및 장치가 적용되기 이전 단계인 연속 변수 양자키 분배(CV-QKD)와 이진 비트키 생성 방법을 간략하게 설명한다.

[0034] 도 5에 도시된 바와 같이, 송신단(10, Alice) 및 수신단(20, Bob)은 이미 공지된 연속 변수 양자키 분배 프로토콜을 통하여 연속된 변수로 구성되어 있는 초기 양자키(Raw Key, X)를 공유한다.

[0035] 이때, 연속 변수 양자키 분배 프로토콜은 양자 채널(Quantum Channel)을 통해 수행되며 양자 채널을 통해 초기 양자키(X)를 분배하는 과정에서 연속 변수 오류(Quantum Error, E)가 발생하게 되어, 연속 변수 양자키 분배(CV-QKD)가 수행되면 송신단(10, Alice)이 보유한 초기 양자키인 송신단측 초기 양자키(X)와 수신단(20, Bob)이 보유한 초기 양자키인 수신단측 초기 양자키(X')는 서로 차이가 발생하게 된다.

[0036] 한편, 송신단측 초기 양자키(X) 및 수신단측 초기 양자키(X') 각각은 연속된 변수로 구성되어 있기 때문에 양자 통신을 위한 암호키로 활용되기는 어려우며, 송신단(10, Alice) 및 수신단(20, Bob) 각각은 자신의 초기 양자키(X, X')를 서로 동일한 규칙으로 양자화하여, 양자 통신을 위한 암호키로 활용될 수 있는 형태인 이진 비트키를 생성한다.

[0037] 이때, 송신단(10, Alice) 및 수신단(20, Bob)이 이진 비트키를 생성하기 위해 활용하는 방법의 일 실시예로는 경판정(Hard Decision) 방법이 있다.

[0038] 이때, 송신단(10, Alice)이 보유하는 이진 비트키는 송신단측 이진 비트키(X_A)로 정의하고, 수신단(20, Bob)이 보유하는 이진 비트키는 수신단측 이진 비트키(X_B)로 정의한다.

[0039] 여기서, 양자 통신을 위해서는 송신단(10, Alice) 및 수신단(20, Bob) 각각이 보유하는 이진 비트키는 서로 동일해야 하나, 연속 변수 양자키 분배(CV-QKD)와 이진 비트키 생성 방법만을 거치는 경우, 양자 채널의 특성 및 이진키 판정의 랜덤성으로 인해 송신단측 이진 비트키(x_A)와 수신단측 이진 비트키(x_B)는 서로 차이가 발생하게 된다.

[0040] 이때, 송신단측 이진 비트키(x_A)와 수신단측 이진 비트키(x_B)의 관계를 수학식으로 표현하면 아래 수학식 1과 같다.

[0041] [수학식 1]

[0042] $$x_B = e' \oplus x_A$$

[0043] 이때, x_B는 수신단측 이진 비트키, x_A는 송신단측 이진 비트키, e'은 이진 비트 오류를 의미한다.

[0044] 이러한, 송신단측 이진 비트키(x_A)와 수신단측 이진 비트키(x_B)를 서로 동일하게 정정하는 과정을 정보 조정(Information Reconciliation)이라 하며, 종래의 대표적인 정보 조정 방법은 슬라이스드 리컨실리에이션 방법이 있다.

[0045] 예를 들어, 본 발명의 실시예에 따른 연속 변수 양자키 분배의 정보 조정을 위한 이진 비트키 추정 방법 및 장치는 정보 조정(Information Reconciliation) 과정에서 송신단측 이진 비트키(X_A)와 수신단측 이진 비트키(X_B)를 서로 동일하게 조정하기 위한 방법 및 장치를 의미할 수 있다.

[0046] 이때, 연속 변수 양자키 분배(CV-QKD)와 이진 비트키 생성 방법에 대한 보다 구체적인 설명은 종래에 공지된 바

와 같으므로 더 이상의 구체적인 설명은 생략하도록 한다.

[0047] 이제 도 2를 참조하여, 본 발명의 실시예에 따른 연속 변수 양자키 분배의 정보 조정을 위한 이진 비트키 추정 장치(200)를 설명한다.

[0048] 도 2는 본 발명의 실시예에 따른, 연속 변수 양자키 분배의 정보 조정을 위한 이진 비트키 추정 장치를 설명하기 위한 구성도이다.

[0049] 도 2에 도시된 바와 같이, 본 발명의 실시예에 따른 연속 변수 양자키 분배의 정보 조정을 위한 이진 비트키 추정 장치(200)는 정보 수신부(210), 오류 산출부(220) 및 이진 비트키 추정부(230)를 포함한다.

[0050] 정보 수신부(210)는 송신단측 이진 비트키(x_A)에 기초하여 생성된 송신 신호(S)를 송신단(10, Alice)으로부터 수신한다.

[0051] 이때, 송신단측 이진 비트키(x_A)는 상술한 바와 같이, 송신단측 초기 양자키(X)를 양자화하여 생성된 암호키를 의미할 수 있다.

[0052] 이때, 송신 신호(S)는 정보 조정을 위하여 송신단(10, Alice)이 생성하여 본 발명의 실시예에 따른 연속 변수 양자키 분배의 정보 조정을 위한 이진 비트키 추정 장치(200)가 포함된 수신단(20, Bob)에 전송하는 신호를 의미할 수 있다.

[0053] 오류 산출부(220)는 송신 신호(S), 미리 저장된 수신단측 이진 비트키(x_B) 및 기설정된 패리티 체크 행렬(Parity Check Matrix, c^T) 중 적어도 하나에 기초하여 송신단측 이진 비트키(x_A)와 수신단측 이진 비트키(x_B) 상호 간의 차이를 나타내는 이진 비트 오류(e')를 산출한다.

[0054] 이때, 수신단측 이진 비트키(x_B)는 상술한 바와 같이, 수신단측 초기 양자키(X')를 양자화하여 생성된 암호키를 의미할 수 있다.

[0055] 이때, 패리티 체크 행렬(Parity Check Matrix, c^T)은 선형 부호(Linear Code)의 패리티 검사를 나타내는 행렬로, 각 행은 패리티 검사를 나타내는 방정식의 계수로 표시되는 행렬을 의미하며, 패리티 체크 행렬에 대한 보다 구체적인 설명은 종래에 공지된 바와 같으므로 생략한다.

[0056] 이진 비트키 추정부(230)는 수신단측 이진 비트키(x_B) 및 이진 비트 오류(e')에 기초하여 송신단측 이진 비트키(x_A)를 추정한다.

[0057] 이때, 송신 신호(S)는, 송신단측 이진 비트키(x_A) 및 미리 선택된 임의의 부호어(Codeword, v)를 XOR 연산하여 생성된 신호이다.

[0058] 이때, 미리 선택된 임의의 부호어(v)는 상술한 패리티 체크 행렬(Parity Check Matrix, c^T)과 곱연산을 하여 0을 만드는 복수의 부호어 중 임의로 선택된 부호어를 의미할 수 있다.

[0059] 예컨대, 미리 선택된 임의의 부호어(v)는 선형 블록 부호(Linear Block Code)에서 정의하는 복수의 부호어(Codeword) 중 임의로 선택된 하나의 부호어를 의미할 수 있다.

[0060] 다시 말해, 미리 선택된 임의의 부호어(v)는 $vc^T=0$를 만족하는 복수의 부호어 중 임의로 선택된 부호어를 의미할 수 있다.

[0061] 예컨대, 오류 산출부(220)는, 송신 신호(S) 및 미리 저장된 수신단측 이진 비트키(x_B)를 XOR 연산하여 제1 연산값을 생성하고, 기설정된 패리티 체크 행렬(c^T)에 제1 연산값을 행렬곱 연산하여 제2 연산값을 생성하고, 미리 저장된 룩업 테이블(Lookup Table)에 기초하여 제2 연산값에 대응되는 이진 비트 오류(e')를 결정한다.

[0062] 예를 들어, 이진 비트키 추정부(230)는, 수신단측 이진 비트키(x_B) 및 이진 비트 오류(e')를 XOR 연산하여 송신단측 이진 비트키(x_A)를 추정한다.

[0063] 본 발명의 실시예에 따른, 연속 변수 양자키 분배의 정보 조정을 위한 이진 비트키 추정 장치(200)에 대한 보다 구체적인 설명은 이하 도 3 내지 도 5를 참조하여 후술하도록 하며, 중복되는 설명은 생략한다.

[0064] 이제, 도 3을 참조하여 본 발명의 실시예에 따른, 연속 변수 양자키 분배의 정보 조정을 위한 이진 비트키 추정 방법을 설명한다.

[0065] 도 3은 본 발명의 실시예에 따른, 연속 변수 양자키 분배의 정보 조정을 위한 이진 비트키 추정 방법을 설명하기 위한 순서도이다.

[0066] 도 3에 도시된 바와 같이, 본 발명의 실시예에 따른, 연속 변수 양자키 분배의 정보 조정을 위한 이진 비트키 추정 방법은 송신단으로부터 송신 신호를 수신하는 단계(S310), 이진 비트 오류를 산출하는 단계(S320) 및 송신단측 이진 비트키를 추정하는 단계(S330)를 포함한다.

[0067] S310 단계는, 정보 수신부(210)가, 송신단측 이진 비트키(x_A)에 기초하여 생성된 송신 신호(S)를 송신단(10, Alice)으로부터 수신하는 단계를 의미한다.

[0068] 예를 들어, 송신 신호(S)는, 송신단측 이진 비트키(x_A) 및 미리 선택된 임의의 부호어(Codeword, v)를 XOR 연산하여 생성된 신호일 수 있다.

[0069] 상술한 바와 같이, 미리 선택된 임의의 부호어(v)는 상술한 패리티 체크 행렬(Parity Check Matrix, c^T)과 곱연산을 하여 0을 만드는 복수의 부호어 중 임의로 선택된 부호어를 의미할 수 있다.

[0070] 예를 들어, S310 단계에서 정보 수신부(210)는 고전 채널(Classical Channel)을 통해 상술한 송신 신호(S)를 수신할 수 있다.

[0071] 예컨대, S310 단계에 앞서 송신단(10, Alice) 및 수신단(20, Bob) 각각은 미리 결정된 이진 비트키(x_A, x_B)를 복수 개 결합하여 미리 결정된 선형 부호(Linear Code)의 길이에 맞춰줄 수 있으나, 본 발명은 이에 한정되지 않는다.

[0072] 이때, S310 단계에서 정보 수신부(210)가 수신한 송신 신호(S)를 수학식으로 표현하면 아래 수학식 2와 같다.

[0073] [수학식 2]

[0074] $$S = v \oplus x_A$$

[0075] 이때, S는 송신 신호, v는 미리 선택된 임의의 부호어, x_A는 송신단측 이진 비트키를 의미한다.

[0076] S320 단계는 오류 산출부(220)가, 송신 신호(S), 미리 저장된 수신단측 이진 비트키(x_B) 및 기설정된 패리티 체크 행렬(Parity Check Matrix, c^T) 중 적어도 하나에 기초하여 송신단측 이진 비트키(x_A)와 상기 수신단측 이진 비트키(x_B) 상호 간의 차이를 나타내는 이진 비트 오류(e')를 산출하는 단계를 의미할 수 있다.

[0077] 이제, 도 4를 참조하여 S320 단계의 일 실시예에 대해 보다 구체적으로 설명한다.

[0078] 도 4는 본 발명의 실시예에 따른, 연속 변수 양자키 분배의 정보 조정을 위한 이진 비트키 추정 방법에서 이진 비트 오류를 산출하는 단계를 설명하기 위한 순서도이다.

[0079] 도 4에 도시된 바와 같이, S320 단계는 S321 단계, S323 단계 및 S325 단계를 포함한다.

[0080] S321 단계는, 오류 산출부(220)가 송신 신호(S) 및 미리 저장된 수신단측 이진 비트키(x_B)를 XOR 연산하여 제1 연산값을 생성하는 단계를 의미할 수 있다.

[0081] 이하, 수학식 3을 참조하여 S321 단계를 통해 생성되는 제1 연산값의 의미에 대해 설명한다.

[0082] [수학식 3]

[0083] $$s \oplus x_B = e' \oplus x_A \oplus v \oplus x_A = e' \oplus v$$

[0084] 이때, $s \oplus x_B$는 제1 연산값, S는 송신 신호, x_B는 수신단측 이진 비트키, e'은 이진 비트 오류, x_A는 송신단측

이진 비트키, v는 미리 선택된 임의의 부호어를 의미한다.

[0085] 상술한 수학식 1에서와 같이, $x_B = e' \oplus x_A$ 관계가 성립하고, 상술한 수학식 2에서와 같이, $s = v \oplus x_A$ 관계가 성립하기 때문에, 제1 연산값($s \oplus x_B$)은 상술한 수학식 3에서와 같이 $e' \oplus x_A \oplus v \oplus x_A$와 등가관계가 성립하게 된다.

[0086] 이때, XOR 연산의 성질에 기초하여 $e' \oplus x_A \oplus v \oplus x_A$을 정리하면, 상술한 수학식 3에서와 같이 $e' \oplus v$가 도출될 수 있다.

[0087] 그 결과, 제1 연산값($s \oplus x_B$)는 이진 비트 오류(e') 및 미리 선택된 임의의 부호어(v) 간의 XOR 연산 결과($e' \oplus v$)와 등가관계가 성립하게 된다.

[0088] S323 단계는, 오류 산출부(220)가 기설정된 패리티 체크 행렬(c^T)에 제1 연산값($s \oplus x_B$)을 행렬곱 연산하여 제2 연산값을 생성하는 단계를 의미할 수 있다.

[0089] 이때, 상술한 바와 같이, 제1 연산값($s \oplus x_B$)과 이진 비트 오류(e') 및 미리 선택된 임의의 부호어(v) 간의 XOR 연산 결과($e' \oplus v$)는 서로 등가 관계인 점을 감안하여 S323 단계를 통해 생성되는 제2 연산값의 의미를 아래 수학식 4를 통해 설명한다.

[0090] [수학식 4]

[0091] $$c^T(e' \oplus v) = c^T e'$$

[0092] 이때, $c^T(e' \oplus v)$는 제2 연산값, c^T는 기설정된 패리티 체크 행렬, e'는 이진 비트 오류, v는 미리 선택된 임의의 부호어를 의미한다.

[0093] 이때, 미리 선택된 임의의 부호어(v)는 패리티 체크 행렬(c^T)과 곱연산을 하여 0을 만드는 복수의 부호어 중 임의로 선택된 부호어이기 때문에, 제2 연산값($c^T(e' \oplus v)$)과 $c^T e'$는 서로 등가관계가 성립하게 된다.

[0094] 예를 들어, 제2 연산값($c^T(e' \oplus v)$)과 $c^T e'$가 서로 동일한 이유는 고전 통신에서 기공지된 신드롬 복호화(Syndrome Decoding) 방법에서와 동일하므로 그 구체적인 설명은 생략한다.

[0095] S325 단계는, 오류 산출부(220)가 미리 저장된 룩업 테이블(Lookup Table)에 기초하여 제2 연산값($c^T(e' \oplus v)$)에 대응되는 이진 비트 오류(e')를 결정하는 단계를 의미할 수 있다.

[0096] 상술한 수학식 4에서와 같이, 제2 연산값($c^T(e' \oplus v)$)은 $c^T e'$와 같은 값이기 때문에, S325 단계에서 오류 산출부(220)에 미리 저장된 룩업 테이블(Lookup Table)은 제2 연산값($c^T e'$)과 이진 비트 오류(e')를 서로 대응되도록 매칭하여 저장한 테이블을 의미할 수 있다.

[0097] 예를 들어, 상술한 룩업 테이블에는 제2 연산값($c^T e'$)이 A인 경우 이진 비트 오류(e')는 a임이 미리 저장될 수 있다.

[0098] 예컨대, 제2 연산값($c^T e'$)은 고전 통신에서 기공지된 복호화 방법인 신드롬 복호화(Syndrom Decoding) 방법에서 정의하는 신드롬(Syndrom)을 의미할 수 있으며, 이 경우 미리 저장된 룩업 테이블은 신드롬 복호화 방법에서 정의하는 신드롬 룩업 테이블을 의미할 수 있으며, 신드롬 복호화 방법에서 신드롬과 신드롬 룩업 테이블을 활용하여 이진 비트 오류(e')를 결정하는 보다 구체적인 방법은 기 공지된 바와 같으므로 그 설명은 생략한다.

[0099] 계속 도 3을 참조하여, S330 단계를 설명한다.

[0100] S330 단계는 이진 비트키 추정부(230)가, 수신단측 이진 비트키(x_B) 및 이진 비트 오류(e')에 기초하여 송신단측 이진 비트키(x_A)를 추정하는 단계를 의미할 수 있다.

[0101] 보다 상세하게, S330 단계는 수신단측 이진 비트키(x_B) 및 이진 비트 오류(e')를 XOR 연산하여 송신단측 이진 비트키(x_A)를 추정하는 단계를 포함할 수 있다.

[0102] 상술한 수학식 1에서와 같이, 수신단측 이진 비트키(x_B) 및 이진 비트 오류(e')를 XOR 연산하면 송신단측 이진 비트키(x_A)가 생성될 수 있다.

[0103] S310 단계, S320 단계 및 S330 단계의 수행 결과 수신단(20, Bob)은 송신단측 이진 비트키(x_A)를 추정할 수 있기 때문에, 송신단(10, Alice) 및 수신단(20, Bob)은 서로 동일한 이진 비트키를 공유할 수 있게 된다.

[0104] 이제 도 5를 참조하여, 본 발명의 실시예에 따른 연속 변수 양자키 분배의 정보 조정을 위한 이진 비트키 추정 방법 및 장치를 계속 설명한다.

[0105] 이때, 본 발명의 실시예에 따른 연속 변수 양자키 분배의 정보 조정을 위한 이진 비트키 추정 장치(200)는 도 5에 도시된 수신단(20, Bob)에 포함될 수 있다.

[0106] 상술한 바와 같이, 연속 변수 양자키 분배를 통하여 송신단(10, Alice) 및 수신단(20, Bob)은 각각은 송신단측 초기 양자키(X)와 수신단측 초기 양자키(X')를 보유하며, 송신단(10, Alice) 및 수신단(20, Bob) 각각은 자신의 초기 양자키(X, X')를 서로 동일한 규칙으로 양자화하여, 양자 통신을 위한 암호키로 활용될 수 있는 형태인 이진 비트키를 생성하며, 그 결과 송신단(10, Alice)은 송신단측 이진 비트키(x_A)를 보유하고, 수신단(20, Bob)은 수신단측 이진 비트키(x_B)를 보유하게 된다.

[0107] 그 뒤, 송신단(10, Alice)은 송신단측 이진 비트키(x_A)와 선형 블록 부호(Linear Block Code)에서 정의하는 복수의 부호어(Codeword) 중 임의로 선택된 하나의 부호어인 미리 선택된 임의의 부호어(v)를 서로 XOR 연산하여 송신 신호(S)를 생성한 뒤, 고전 채널을 통해 송신 신호(S)를 수신단(20, Bob)에 전송한다.

[0108] 그 뒤, 수신단(20, Bob)은 송신 신호(S) 및 수신단측 이진 비트키(x_B)를 서로 XOR 연산하여 제1 연산값($e' \oplus v$)을 생성하고, 제1 연산값($e' \oplus v$)에 신드롬 복호화 방법을 적용하여 이진 비트 오류(e')를 결정할 수 있으며, 그 뒤, 수신단(20, Bob)은 수신단측 이진 비트키(x_B)와 이진 비트 오류(e')를 서로 XOR 연산하여 송신단측 이진 비트키(x_A)를 추정할 수 있다.

[0109] 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

[0110] 10: 송신단(Alice)

20: 수신단(Bob)

200: 연속 변수 양자키 분배의 정보 조정을 위한 이진 비트키 추정 장치

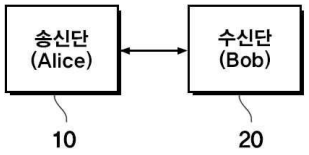
210: 정보 수신부

220: 오류 산출부

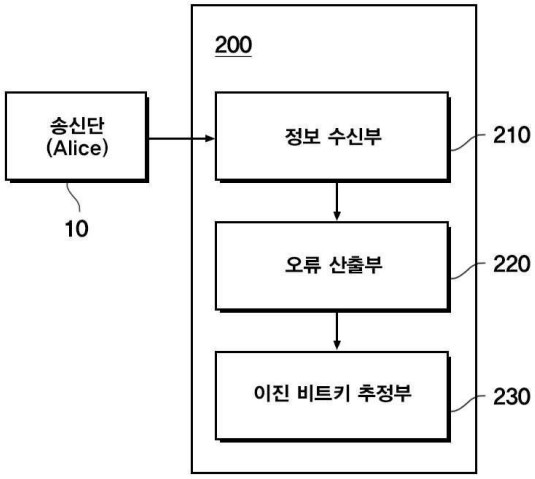
230: 이진 비트키 추정부

도면

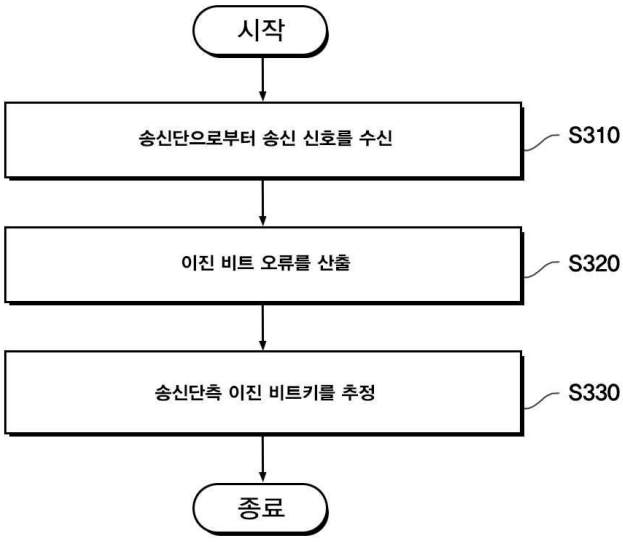
도면1



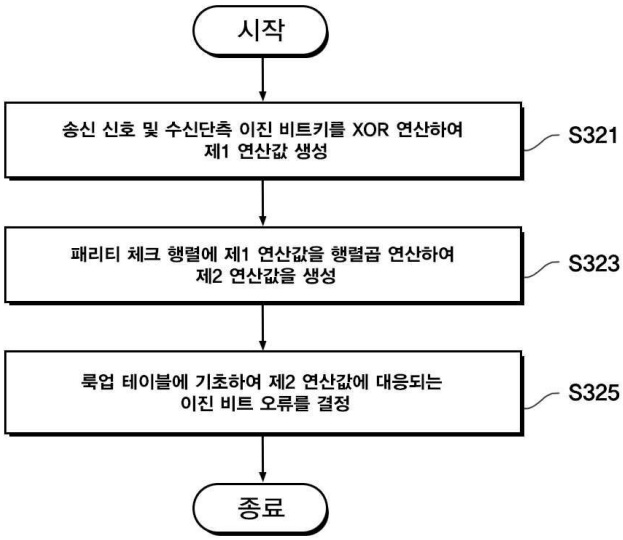
도면2



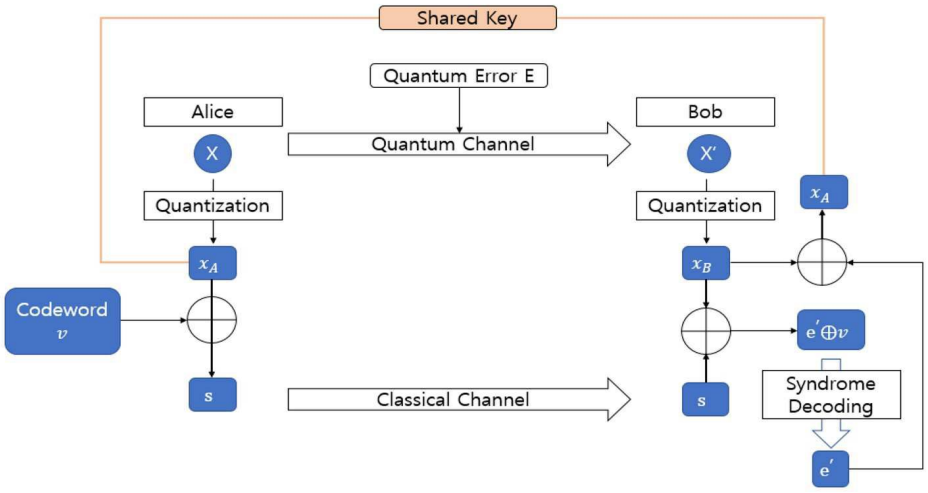
도면3



도면4


시작
송신 신호 및 수신단측 이진 비트키를 XOR 연산하여 제1 연산값 생성
S321
패리티 체크 행렬에 제1 연산값을 행렬곱 연산하여 제2 연산값을 생성
S323
룩업 테이블에 기초하여 제2 연산값에 대응되는 이진 비트 오류를 결정
S325
종료

도면5


Shared Key
Quantum Error E
Alice
Bob
Quantum Channel
X
X'
Quantization
Quantization
x_A
x_B
x_A
Codeword
v
$e' \oplus v$
s
s
Classical Channel
Syndrome Decoding
e'