(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2024-0124105
(43) 공개일자 2024년08월16일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *H04B 10/079* (2013.01)
(52) CPC특허분류
H04L 9/0852 (2023.08)
H04B 10/07953 (2013.01)
(21) 출원번호 10-2023-0016940
(22) 출원일자 2023년02월08일
심사청구일자 2023년02월08일

(71) 출원인
국방과학연구소
대전광역시 유성구 북유성대로488번길 160 (수남동)
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
박주윤
서울특별시 성북구 안암로 145
김범일
서울특별시 성북구 안암로 145
허준
서울특별시 성북구 안암로 145
(74) 대리인
특허법인 광장리앤고

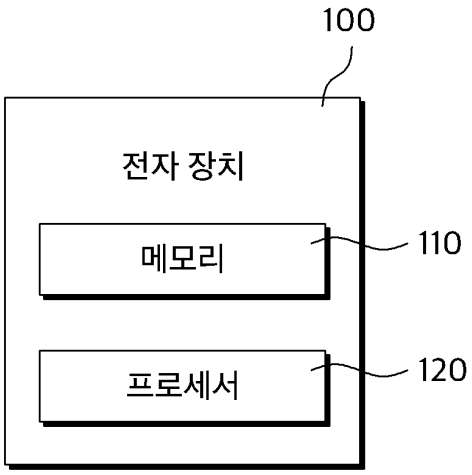
전체 청구항 수 : 총 11 항

(54) 발명의 명칭 **양자직접통신의 통계적 분석 방법 및 그 전자 장치**

(57) 요 약

본 개시의 전자 장치의 양자직접통신의 통계적 분석 방법으로서, 양자직접통신을 위한 프로토콜에 따른 도청에 의해 간섭 받는 양자직접통신에 관한 시뮬레이션을 수행하는 단계; 시뮬레이션 결과를 기초로, 평균광자수(Mean Photon Number)가 제1값인 신호 상태(signal state)일 때 시뮬레이션에서의 수신 장치가 생성한 레이저 펄스에 포함되는 제1광자가 제1경로를 통해 수신 장치에서 검출되는 확률에 관한 제1정보, 제1광자가 제2경로를 통해 도청을 수행하는 도청 장치에서 검출되는 확률에 관한 제2정보, 및 에러율에 관한 정보를 확인하는 단계; 및 가우시안 근사(Gaussian Approximation)을 이용하여 제1정보, 제2정보, 및 에러율에 관한 정보의 상한 및 하한 중 적어도 하나를 계산하고, 제1정보, 제2정보, 및 에러율에 관한 정보의 상한 및 하한 중 적어도 하나에 기초하여 프로토콜의 보안 용량(Secrecy Capacity)을 계산하는 단계를 포함하는 통계적 분석 방법이 제공될 수 있다.

대 표 도 - 도1



명 세 서

청구범위

청구항 1

전자 장치의 양자직접통신의 통계적 분석 방법으로서,

양자직접통신을 위한 프로토콜에 따른 도청에 의해 간섭 받는 양자직접통신에 관한 시뮬레이션을 수행하는 단계;

상기 시뮬레이션 결과를 기초로, 평균광자수(Mean Photon Number)가 제1값인 신호 상태(signal state)일 때 상기 시뮬레이션에서의 수신 장치가 생성한 레이저 펄스에 포함되는 제1광자가 제1경로를 통해 상기 수신 장치에서 검출되는 확률에 관한 제1정보, 상기 제1광자가 제2경로를 통해 상기 도청을 수행하는 도청 장치에서 검출되는 확률에 관한 제2정보, 및 에러율에 관한 정보를 확인하는 단계; 및

가우시안 근사(Gaussian Approximation)를 이용하여 상기 제1정보, 제2정보, 및 에러율에 관한 정보의 상한 및 하한 중 적어도 하나를 계산하고, 상기 제1정보, 제2정보, 및 에러율에 관한 정보의 상한 및 하한 중 적어도 하나에 기초하여 상기 프로토콜의 보안 용량(Secrecy Capacity)을 계산하는 단계를 포함하는, 통계적 분석 방법.

청구항 2

제1항에 있어서,

상기 제1경로는,

상기 제1광자가 상기 수신 장치로부터 상기 시뮬레이션에서의 송신 장치를 거쳐 상기 수신 장치로 전송되는 경로를 포함하고,

상기 제2경로는,

상기 제1광자가 상기 수신 장치로부터 상기 송신 장치를 거쳐 상기 도청 장치로 전송되는 경로를 포함하는, 통계적 분석 방법.

청구항 3

제1항에 있어서,

상기 제2정보는,

상기 제2경로를 통해 상기 도청 장치에서 상기 제1광자가 제1개수 검출되는 확률에 관한 제2-1정보, 상기 제2경로를 통해 상기 도청 장치에서 상기 제1광자가 제2개수 검출되는 확률에 관한 제2-2정보, 및 상기 제2경로를 통해 상기 도청 장치에서 상기 제1광자가 적어도 제3개수 검출되는 확률에 관한 제2-3정보를 포함하고,

상기 에러율에 관한 정보는,

DBER(Detection Bit Error Rate)에 관한 정보의 제1상한, 및 QBER(Quantum Bit Error Rate)에 관한 정보를 포함하고,

상기 계산하는 단계는,

가우시안 근사를 이용하여 상기 제1정보의 하한, 상기 QBER에 관한 정보의 상한, 상기 제2-1정보의 하한, 상기 제2-2정보의 하한, 상기 제2-3정보의 상한, 및 상기 DBER에 관한 정보의 제2상한을 계산하고, 상기 제1정보의 하한, 상기 QBER에 관한 정보의 상한, 상기 제2-1정보의 하한, 상기 제2-2정보의 하한, 상기 제2-3정보의 상한, 및 상기 DBER에 관한 정보의 제2상한에 기초하여 상기 프로토콜의 보안 용량을 계산하는 단계를 포함하는, 통계적 분석 방법.

청구항 4

제3항에 있어서,

상기 계산하는 단계는,

기 설정된 추정 실패 확률(Failure Probability) 및 표준 정규 분포(Standard Normal Distribution)의 역누적 분포함수(Inverse Cumulative Distribution Function)에 기초하여 신뢰도를 계산하고, 상기 신뢰도에 기초하여 상기 제1정보의 하한, 상기 QBER에 관한 정보의 상한, 상기 제2-1정보의 하한, 상기 제2-2정보의 하한, 상기 제2-3정보의 상한, 및 상기 DBER에 관한 정보의 제2상한을 계산하는 단계를 포함하는, 통계적 분석 방법.

청구항 5

제3항에 있어서,

상기 제2-1정보는,

상기 신호 상태일 때 상기 수신 장치가 생성한 레이저 펄스에 상기 제1광자가 상기 제1개수 포함될 확률에 관한 제1포아송 정보, 상기 수신 장치에서 상기 제1개수의 상기 제1광자가 생성되어 상기 시뮬레이션에서의 송신 장치로 전송된 경우 상기 송신 장치에서 상기 제1광자가 검출되는 확률에 관한 제1산출 정보의 제1하한, 및 상기 수신 장치에서 상기 제1광자가 생성되지 않았음에도 상기 송신 장치에서 상기 제1광자가 검출된 것으로 판단한 확률에 관한 제3산출 정보를 기초로 계산되고,

상기 제2-2정보는,

상기 신호 상태일 때 상기 수신 장치가 생성한 레이저 펄스에 상기 제1광자가 상기 제2개수 포함될 확률에 관한 제2포아송 정보, 및 상기 수신 장치에서 상기 제2개수의 상기 제1광자가 생성되어 상기 송신 장치로 전송된 경우 상기 송신 장치에서 상기 제1광자가 검출되는 확률에 관한 제2산출 정보의 제1하한, 및 상기 제3산출 정보를 기초로 계산되고,

상기 제2-3정보는,

상기 제2-1정보 및 상기 제2-2정보를 기초로 계산되는, 통계적 분석 방법.

청구항 6

제5항에 있어서,

상기 제3산출 정보는,

상기 수신 장치 및 상기 송신 장치의 기 설정된 다크 카운트율(Dark Count Rate)인, 통계적 분석 방법.

청구항 7

제5항에 있어서,

상기 확인하는 단계는,

상기 시뮬레이션 결과를 기초로, 평균광자수가 제2-1값인 제1미끼 상태일 때 상기 수신 장치가 생성한 레이저 펄스에 포함되는 제2-1광자가 제3경로를 통해 상기 수신 장치에서 검출되는 확률에 관한 제3-1정보, 평균광자수가 제2-2값인 제2미끼 상태일 때 상기 수신 장치가 생성한 레이저 펄스에 포함되는 제2-2광자가 상기 제3경로를 통해 상기 수신 장치에서 검출되는 확률에 관한 제3-2정보, 및 평균광자수가 제2-3값인 제3미끼 상태일 때 상기 수신 장치가 생성한 레이저 펄스에 포함되는 제2-3광자가 상기 제3경로를 통해 상기 수신 장치에서 검출되는 확률에 관한 제3-3정보를 확인하고, 상기 제1광자가 상기 제3경로를 통해 상기 수신 장치에서 검출되는 확률에 관한 제4정보를 확인하는 단계를 포함하고,

상기 제3경로는,

상기 제2-1광자, 제2-2광자, 및 제2-3광자가 상기 수신 장치로부터 상기 도청 장치를 거치지 않고 상기 송신 장치로 전송되는 경로를 포함하고,

상기 제2-1정보의 하한은,

상기 제1산출 정보의 제2하한을 기초로 계산되고,

상기 제2-2정보의 하한은,

상기 제2산출 정보의 제2하한을 기초로 계산되고,

상기 제1산출 정보의 제2하한은,

상기 제1값, 상기 제2-2값, 상기 제2-3값, 상기 제3-2정보의 하한, 상기 제3-3정보의 상한, 상기 제4정보의 상한, 및 상기 제3산출 정보를 기초로 계산되고,

상기 제2산출 정보의 제2하한은,

상기 제1값, 상기 제2-1값, 상기 제2-2값, 상기 제3-1정보의 하한, 상기 제3-2정보의 상한, 상기 제4정보의 상한, 및 상기 제3산출 정보를 기초로 계산되는, 통계적 분석 방법.

청구항 8

제7항에 있어서,

상기 제1정보, 제3-1정보, 제3-2정보, 및 제3-3정보는,

복수의 파라미터들을 기초로 확인되고,

상기 복수의 파라미터들은,

기 설정된 개수의 광자, 상기 기 설정된 개수의 광자에 대한 상기 제1광자의 개수의 비율, 상기 기 설정된 개수의 광자에 대한 상기 제2-1광자의 개수의 비율, 상기 기 설정된 개수의 광자에 대한 상기 제2-2광자의 개수의 비율, 상기 기 설정된 개수의 광자에 대한 상기 제2-3광자의 개수의 비율, 상기 기 설정된 개수의 광자에 대한 평균광자수가 제2-4값인 제4미끼 상태일 때 상기 수신 장치가 생성한 레이저 펄스에 포함되는 제2-4광자의 개수의 비율, 상기 제1값, 상기 제2-1값, 상기 제2-2값, 상기 제2-3값, 및 상기 제2-4값을 포함하고,

상기 시뮬레이션을 수행하는 단계는,

기 설정된 제한 조건을 만족하면서 상기 보안 용량이 최대가 되도록 하는 상기 복수의 파라미터들을 확인하기 위해 양자직접통신에 관한 시뮬레이션을 수행하는 단계를 포함하는, 통계적 분석 방법.

청구항 9

제7항에 있어서,

상기 DBER에 관한 정보는,

제1DBER에 관한 정보 및 제2DBER에 관한 정보를 포함하고,

상기 제1DBER에 관한 정보의 제1상한은,

상기 제1산출 정보의 제1하한, 상기 제2-3값, 상기 제2-3광자를 상기 제3경로를 통해 전송할 경우의 BER(Bit Error Rate)에 관한 정보, 상기 제3-3정보, 및 상기 제3산출 정보를 기초로 계산되고,

상기 제2DBER에 관한 정보의 제1상한은,

상기 제2산출 정보의 제1하한, 상기 제2-2값, 상기 제2-3값, 상기 제2-2광자를 상기 제3경로를 통해 전송할 경우의 BER에 관한 정보, 상기 제3-2정보, 상기 제2-3광자를 상기 제3경로를 통해 전송할 경우의 BER에 관한 정보, 상기 제3-3정보, 및 상기 제3산출 정보를 기초로 계산되고,

상기 제1DBER에 관한 정보의 제2상한은,

상기 제1산출 정보의 제2하한, 상기 제2-3값, 상기 제2-3광자를 상기 제3경로를 통해 전송할 경우의 BER에 관한 정보의 상한, 상기 제3-3정보의 상한, 및 상기 제3산출 정보를 기초로 계산되고,

상기 제2DBER에 관한 정보의 제2상한은,

상기 제2산출 정보의 제2하한, 상기 제2-2값, 상기 제2-3값, 상기 제2-2광자를 상기 제3경로를 통해 전송할 경우의 BER에 관한 정보의 상한, 상기 제3-2정보의 상한, 상기 제2-3광자를 상기 제3경로를 통해 전송할 경우의 BER에 관한 정보의 하한, 상기 제3-3정보의 하한, 및 상기 제3산출 정보를 기초로 계산되는, 통계적 분석 방법.

청구항 10

양자직접통신의 통계적 분석을 위한 전자 장치로서,

적어도 하나의 프로그램이 저장된 메모리; 및

상기 적어도 하나의 프로그램을 실행함으로써, 양자직접통신을 위한 프로토콜에 따른 도청에 의해 간섭 받는 양자직접통신에 관한 시뮬레이션을 수행하고,

상기 시뮬레이션 결과를 기초로, 평균광자수(Mean Photon Number)가 제1값인 신호 상태(signal state)일 때 상기 시뮬레이션에서의 수신 장치가 생성한 레이저 펄스에 포함되는 제1광자가 제1경로를 통해 상기 수신 장치에서 검출되는 확률에 관한 제1정보, 상기 제1광자가 제2경로를 통해 상기 도청을 수행하는 도청 장치에서 검출되는 확률에 관한 제2정보, 및 에러율에 관한 정보를 확인하고,

가우시안 근사(Gaussian Approximation)를 이용하여 상기 제1정보, 제2정보, 및 에러율에 관한 정보의 상한 및 하한 중 적어도 하나를 계산하고, 상기 제1정보, 제2정보, 및 에러율에 관한 정보의 상한 및 하한 중 적어도 하나에 기초하여 상기 프로토콜의 보안 용량(Secrecy Capacity)을 계산하는 프로세서를 포함하는, 전자 장치.

청구항 11

양자직접통신의 통계적 분석 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 비일시적 기록매체로서,

상기 통계적 분석 방법은,

양자직접통신을 위한 프로토콜에 따른 도청에 의해 간섭 받는 양자직접통신에 관한 시뮬레이션을 수행하는 단계;

상기 시뮬레이션 결과를 기초로, 평균광자수(Mean Photon Number)가 제1값인 신호 상태일 때 상기 시뮬레이션에서의 수신 장치가 생성한 레이저 펄스에 포함되는 제1광자가 제1경로를 통해 상기 수신 장치에서 검출되는 확률에 관한 제1정보, 상기 제1광자가 제2경로를 통해 상기 도청을 수행하는 도청 장치에서 검출되는 확률에 관한 제2정보, 및 에러율에 관한 정보를 확인하는 단계; 및

가우시안 근사(Gaussian Approximation)를 이용하여 상기 제1정보, 제2정보, 및 에러율에 관한 정보의 상한 및 하한 중 적어도 하나를 계산하고, 상기 제1정보, 제2정보, 및 에러율에 관한 정보의 상한 및 하한 중 적어도 하나에 기초하여 상기 프로토콜의 보안 용량(Secrecy Capacity)을 계산하는 단계를 포함하는, 비일시적 기록매체.

발명의 설명

기 술 분 야

[0001] 본 개시는 양자직접통신의 통계적 분석 방법 및 그 전자 장치에 관한 것이다.

배 경 기 술

[0002] 양자직접통신은 양자키분배(Quantum Key Distribution)와 달리 양자 채널의 상황을 파악하여 보내고자 하는 메시지를 직접 암호화하여 전송하는 방법이다.

[0003] 양자직접통신에서의 보안 용량(Secrecy Capacity)은 도청자가 전송된 비밀 정보에 대하여 무시할 수 있는 정보만을 취할 수 있도록 보장하면서 양자 채널을 통해 송신자가 수신자에게 전달할 수 있는 점근적 정보율(asymptotic information rate)을 정의한다. 비특허문헌(Dong Pan, Zaisheng Lin, Jiawei Wu, Haoran Zhang, Zhen Sun, Dong Ruan, Liugo Yin, and Gui Lu Long, "Experimental free-space quantum secure direct communication and its security analysis,"Photon. Res. 8, 1522-1531 (2020))과 같은 양자직접통신의 보안 용량(Secrecy Capacity)을 분석하는 종래의 방법들은 유한한 데이터 사이즈를 사용할 때 발생하는 통계적 변동(Statistical Fluctuation)을 고려하지 않았다. 따라서, 실용적인 양자직접통신을 구현하기 위해 데이터 사이즈에 따른 양자직접통신의 프로토콜의 보안 용량을 분석하는 방법이 요구된다.

발명의 내용

해결하려는 과제

[0004] 개시된 실시예들은 양자직접통신의 통계적 분석 방법 및 그 전자 장치를 개시하고자 한다. 본 실시예가 이루고

자 하는 기술적 과제는 상기된 바와 같은 기술적 과제들로 한정되지 않으며, 이하의 실시예들로부터 또 다른 기술적 과제들이 유추될 수 있다.

과제의 해결 수단

[0005] 일 실시예에 따른 전자 장치의 양자직접통신의 통계적 분석 방법으로서, 양자직접통신을 위한 프로토콜에 따른 도청에 의해 간섭 받는 양자직접통신에 관한 시뮬레이션을 수행하는 단계; 시뮬레이션 결과를 기초로, 평균광자수(Mean Photon Number)가 제1값인 신호 상태(signal state)일 때 시뮬레이션에서의 수신 장치가 생성한 레이저 펄스에 포함되는 제1광자가 제1경로를 통해 수신 장치에서 검출되는 확률에 관한 제1정보, 제1광자가 제2경로를 통해 도청을 수행하는 도청 장치에서 검출되는 확률에 관한 제2정보, 및 에러율에 관한 정보를 확인하는 단계; 가우시안 근사(Gaussian Approximation)를 이용하여 제1정보, 제2정보, 및 에러율에 관한 정보의 상한 및 하한 중 적어도 하나를 계산하고, 제1정보, 제2정보, 및 에러율에 관한 정보의 상한 및 하한 중 적어도 하나에 기초하여 프로토콜의 보안 용량(Secrecy Capacity)을 계산하는 단계를 포함하는 통계적 분석 방법이 제공될 수 있다.

[0006] 일 실시예에 따른 전자 장치의 양자직접통신의 통계적 분석 방법으로서, 제1경로는, 제1광자가 수신 장치로부터 시뮬레이션의 송신 장치를 거쳐 수신 장치로 전송되는 경로를 포함하고, 제2경로는, 제1광자가 수신 장치로부터 송신 장치를 거쳐 도청 장치로 전송되는 경로를 포함하는 통계적 분석 방법이 제공될 수 있다.

[0007] 일 실시예에 따른 전자 장치의 양자직접통신의 통계적 분석 방법으로서, 제2정보는, 제2경로를 통해 도청 장치에서 제1광자가 제1개수 검출되는 확률에 관한 제2-1정보, 제2경로를 통해 도청 장치에서 제1광자가 제2개수 검출되는 확률에 관한 제2-2정보, 및 제2경로를 통해 도청 장치에서 제1광자가 적어도 제3개수 검출되는 제2-3정보를 포함하고, 에러율에 관한 정보는, DBER(Detection Bit Error Rate)에 관한 정보의 제1상한, 및 QBER(Quantum Bit Error Rate)에 관한 정보를 포함하고, 계산하는 단계는, 가우시안 근사를 이용하여 제1정보의 하한, QBER에 관한 정보의 상한, 제2-1정보의 하한, 제2-3정보의 상한, 및 DBER에 관한 정보의 제2상한을 계산하고, 제1정보의 하한, QBER에 관한 정보의 상한, 제2-1정보의 하한, 제2-2정보의 하한, 제2-3정보의 상한, 및 DBER에 관한 정보의 제2상한에 기초하여 프로토콜의 보안 용량을 계산하는 단계를 포함하는 통계적 분석 방법이 제공될 수 있다.

[0008] 일 실시예에 따른 전자 장치의 양자직접통신을 위한 통계적 분석 방법으로서, 계산하는 단계는, 기 설정된 추정 실패 확률(Failure Probability) 및 표준 정규 분포(Standard Normal Distribution)의 역누적분포함수(Inverse Cumulative Distribution Function)에 기초하여 신뢰도를 계산하고, 신뢰도에 기초하여 제1정보의 하한, QBER에 관한 정보의 상한, 제2-1정보의 하한, 제2-2정보의 하한, 제2-3정보의 상한, 및 상기 DBER에 관한 정보의 제2상한을 계산하는 단계를 포함하는 통계적 분석 방법이 제공될 수 있다.

[0009] 일 실시예에 따른 전자 장치의 양자직접통신을 위한 통계적 분석 방법으로서, 제2-1정보는, 신호 상태일 때 수신 장치가 생성한 레이저 펄스에 제1광자가 제1개수 포함될 확률에 관한 제1포아송 정보, 수신 장치에서 제1개수의 제1광자가 생성되어 시뮬레이션의 송신 장치로 전송된 경우 송신 장치에서 제1광자가 검출되는 확률에 관한 제1산출 정보의 제1하한, 및 수신 장치에서 제1광자가 생성되지 않았음에도 송신 장치에서 제1광자가 검출된 것으로 판단한 확률에 관한 제3산출 정보를 기초로 계산되고, 제2-2정보는, 신호 상태일 때 수신 장치가 생성한 레이저 펄스에 제1광자가 제2개수 포함될 확률에 관한 제2포아송 정보, 및 수신 장치에서 제2개수의 제1광자가 생성되어 송신 장치로 전송된 경우 송신 장치에서 제1광자가 검출되는 확률에 관한 제2산출 정보의 제1하한, 및 제3산출 정보를 기초로 계산되고, 제2-3정보는, 제2-1정보 및 제2-2정보를 기초로 계산되는 통계적 분석 방법이 제공될 수 있다.

[0010] 일 실시예에 따른 전자 장치의 양자직접통신을 위한 통계적 분석 방법으로서, 제3산출 정보는, 수신 장치 및 송신 장치의 기 설정된 다크 카운트율(Dark Count Rate)인 통계적 분석 방법이 제공될 수 있다.

[0011] 일 실시예에 따른 전자 장치의 양자직접통신을 위한 통계적 분석 방법으로서, 확인하는 단계는, 시뮬레이션 결과를 기초로, 평균광자수가 제2-1값인 제1미끼 상태일 때 수신 장치가 생성한 레이저 펄스에 포함되는 제2-1광자가 제3경로를 통해 수신 장치에서 검출되는 확률에 관한 제3-1정보, 평균광자수가 제2-2값인 제2미끼 상태일 때 수신 장치가 생성한 레이저 펄스에 포함되는 제2-2광자가 제3경로를 통해 수신 장치에서 검출되는 확률에 관한 제3-2정보, 및 평균광자수가 제2-3값인 제3미끼 상태일 때 수신 장치가 생성한 레이저 펄스에 포함되는 제2-3광자가 제3경로를 통해 수신 장치에서 검출되는 확률에 관한 제3-3정보를 확인하고, 제1광자가 제3경로를 통해 수신 장치에서 검출되는 확률에 관한 제4정보를 확인하는 단계를 포함하고, 제3경로는 제2-1광자, 제2-2광자,

및 제2-3광자가 수신 장치로부터 도청 장치를 거치지 않고 송신 장치로 전송되는 경로를 포함하고, 제2-1정보의 하한은, 제1산출 정보의 제2하한을 기초로 계산되고, 제2-2정보의 하한은, 제2산출 정보의 제2하한을 기초로 계산되고, 제1산출 정보의 제2하한은, 제1값, 제2-2값, 제2-3값, 제3-2정보의 하한, 제3-3정보의 상한, 제4정보의 상한, 및 제3산출 정보를 기초로 계산되고, 제2산출 정보의 제2하한은, 제1값, 제2-2값, 제3-1정보의 하한, 제3-2정보의 상한, 제4정보의 상한, 및 제3산출 정보를 기초로 계산되는 통계적 분석 방법이 제공될 수 있다.

[0012] 일 실시예에 따른 전자 장치의 양자직접통신을 위한 통계적 분석 방법으로서, 제1정보, 제3-1정보, 제3-2정보, 및 제3-3정보는, 복수의 파라미터들을 기초로 확인되고, 복수의 파라미터들은, 기 설정된 개수의 광자, 기 설정된 개수의 광자에 대한 제1광자의 개수의 비율, 기 설정된 개수의 광자에 대한 제2-1광자의 개수의 비율, 기 설정된 개수의 광자에 대한 제2-2광자의 개수의 비율, 기 설정된 개수의 광자에 대한 평균광자수가 제2-4값인 제4 미끼 상태일 때 수신 장치가 생성한 레이저 펄스에 포함되는 제2-4광자의 개수의 비율, 제1값, 제2-1값, 제2-2값, 제2-3값, 및 제2-4값을 포함하고, 시뮬레이션을 수행하는 단계는, 기 설정된 제한 조건을 만족하면서 보안 용량이 최대가 되도록 하는 복수의 파라미터들을 확인하기 위해 양자직접통신에 관한 시뮬레이션을 수행하는 단계를 포함하는 통계적 분석 방법이 제공될 수 있다.

[0013] 일 실시예에 따른 전자 장치의 양자직접통신을 위한 통계적 분석 방법으로서, DBER에 관한 정보는, 제1DBER에 관한 정보 및 제2DBER에 관한 정보를 포함하고, 제1DBER에 관한 정보의 제1상한은, 제1산출 정보의 제1하한, 제2-3값, 제2-3광자를 제3경로를 통해 전송할 경우의 BER(Bit Error Rate)에 관한 정보, 제3-3정보, 및 제3산출 정보를 기초로 계산되고, 제2DBER에 관한 정보의 제1상한은, 제2산출 정보의 제1하한, 제2-2값, 제2-3값, 제2-2광자를 제3경로를 통해 전송할 경우의 BER에 관한 정보, 제3-2정보, 제2-3광자를 제3경로를 통해 전송할 경우의 BER에 관한 정보, 제3-3정보, 및 제3산출 정보를 기초로 계산되고, 제1DBER에 관한 정보의 제2상한은, 제1산출 정보의 제2하한, 제2-3값, 제2-3광자를 제3경로를 통해 전송할 경우의 BER에 관한 정보의 상한, 제3-3정보의 상한, 및 제3산출 정보를 기초로 계산되고, 제2DBER에 관한 정보의 제2상한은, 제2산출 정보의 하한, 제2-2값, 제2-3값, 제2-2광자를 제3경로를 통해 전송할 경우의 BER에 관한 정보의 상한, 제3-2정보의 상한, 제2-3광자를 제3경로를 통해 전송할 경우의 BER에 관한 정보의 하한, 제3-3정보의 하한, 및 제3산출 정보를 기초로 계산되는 통계적 분석 방법이 제공될 수 있다.

[0014] 일 실시예에 따른 양자직접통신의 통계적 분석을 위한 전자 장치로서, 적어도 하나의 프로그램이 저장된 메모리; 및 적어도 하나의 프로그램을 실행함으로써, 양자직접통신을 위한 프로토콜에 따른 도청에 의해 간섭받는 양자직접통신에 관한 시뮬레이션을 수행하고, 시뮬레이션 결과를 기초로, 평균광자수(Mean Photon Number)가 제1값인 신호 상태(signal state)일 때 시뮬레이션에서의 수신 장치가 생성한 레이저 펄스에 포함되는 제1광자가 제1경로를 통해 수신 장치에서 검출되는 확률에 관한 제1정보, 제1광자가 제2경로를 통해 도청을 수행하는 도청 장치에서 검출되는 확률에 관한 제2정보, 및 에러율에 관한 정보를 확인하고, 가우시안 근사(Gaussian Approximation)를 이용하여 제1정보, 제2정보, 및 에러율에 관한 정보의 상한 및 하한 중 적어도 하나를 계산하고, 제1정보, 제2정보, 및 에러율에 관한 정보의 상한 및 하한 중 적어도 하나에 기초하여 프로토콜의 보안 용량(Secrecy Capacity)을 계산하는 프로세서를 포함하는 전자 장치가 제공될 수 있다.

[0015] 일 실시예에 따른 양자직접통신의 통계적 분석 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 비일시적 기록매체로서, 통계적 분석 방법은, 양자직접통신을 위한 프로토콜에 따른 도청에 의해 간섭 받는 양자직접통신에 관한 시뮬레이션을 수행하는 단계; 시뮬레이션 결과를 기초로, 평균광자수(Mean Photon Number)가 제1값인 신호 상태일 때 시뮬레이션에서의 수신 장치가 생성한 레이저 펄스에 포함되는 제1광자가 제1경로를 통해 수신 장치에서 검출되는 확률에 관한 제1정보, 제1광자가 제2경로를 통해 도청을 수행하는 도청 장치에서 검출되는 확률에 관한 제2정보, 및 에러율에 관한 정보를 확인하는 단계; 및 가우시안 근사(Gaussian Approximation)를 이용하여 제1정보, 제2정보, 및 에러율에 관한 정보의 상한 및 하한 중 적어도 하나를 계산하고, 제1정보, 제2정보, 및 에러율에 관한 정보의 상한 및 하한 중 적어도 하나에 기초하여 프로토콜의 보안 용량(Secrecy Capacity)을 계산하는 단계를 포함하는 비일시적 기록매체가 제공될 수 있다.

발명의 효과

[0016] 본 개시에 따르면 전자 장치는 양자직접통신에 관한 시뮬레이션을 수행하고, 시뮬레이션 결과를 기초로 제1정보, 제2정보, 및 에러율에 관한 정보를 확인하고, 가우시안 근사를 이용하여 제1정보, 제2정보, 및 에러율에 관한 정보 각각의 상한(Upper Bound) 및 하한(Lower Bound) 중 적어도 하나를 계산하여 프로토콜의 보안 용량을 계산할 수 있다. 전자 장치는 유한한 데이터 사이즈를 사용할 때 발생하는 통계적 변동을 고려하여 보안 용량을 계산하므로 보다 실용적인 양자직접통신 구현이 가능할 수 있다.

[0017] 발명의 효과는 이상에서 언급된 효과로 제한되지 않으며, 언급되지 않은 또 다른 효과들은 청구범위의 기재로부터 당해 기술분야의 통상의 기술자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[0018] 도 1은 일 실시예에 따른 전자 장치를 나타낸다.

도 2a는 일 실시예에 따른 시뮬레이션의 실제 모델인 양자직접통신 실험의 구성도를 나타낸다.

도 2b는 일 실시예에 따른 위상 인코딩부 및 간섭계부 간의 관계를 나타낸다.

도 3은 일 실시예에 따라 계산된 보안 용량의 그래프를 나타낸다.

도 4는 일 실시예에 따른 전자 장치의 동작 방법을 나타낸다.

발명을 실시하기 위한 구체적인 내용

[0019] 실시예들에서 사용되는 용어는 본 개시에서의 기능을 고려하면서 가능한 현재 널리 사용되는 일반적인 용어들을 선택하였으나, 이는 당 분야에 종사하는 기술자의 의도 또는 판례, 새로운 기술의 출현 등에 따라 달라질 수 있다. 또한, 특정한 경우는 출원인이 임의로 선정한 용어도 있으며, 이 경우 해당되는 설명 부분에서 상세히 그 의미를 기재할 것이다. 따라서 본 개시에서 사용되는 용어는 단순한 용어의 명칭이 아닌, 그 용어가 가지는 의미와 본 개시의 전반에 걸친 내용을 토대로 정의되어야 한다.

[0020] 명세서 전체에서 어떤 부분이 어떤 구성요소를 "포함" 한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있음을 의미한다. 또한, 명세서에 기재된 "..부", "..모듈" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어 또는 소프트웨어로 구현되거나 하드웨어와 소프트웨어의 결합으로 구현될 수 있다.

[0021] 명세서 전체에서 기재된 "a, b, 및 c 중 적어도 하나"의 표현은, 'a 단독', 'b 단독', 'c 단독', 'a 및 b', 'a 및 c', 'b 및 c', 또는 'a,b,c 모두'를 포괄할 수 있다.

[0022] 명세서 전체에서 기재된 "밥(Bob), 엘리스(Alice), 이브(Eavesdropper)"의 표현은, 양자직접통신에 관한 시뮬레이션에서의 수신 장치, 송신 장치, 도청 장치 각각을 의미할 수 있다.

[0023] 아래에서는 첨부한 도면을 참고하여 본 개시의 실시예에 대하여 본 개시가 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 개시는 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다.

[0024] 도 1은 본 개시에 따른 전자 장치(100)를 나타낸다.

[0025] 전자 장치(100)는 메모리(110) 및 프로세서(120)를 포함한다. 도 1에 도시된 전자 장치(100)에는 본 실시예들과 관련된 구성요소들만이 도시되어 있다. 따라서, 전자 장치(100)에는 도 1에 도시된 구성요소들 외에 다른 범용적인 구성요소들이 더 포함될 수 있음은 당해 기술분야의 통상의 기술자에게 자명하다.

[0026] 전자 장치(100)는 양자직접통신을 위한 프로토콜의 보안 용량(Secrecy Capacity)을 계산할 수 있다. 예를 들어, 전자 장치(100)는 가우시안 근사를 이용하여 DL04 프로토콜의 보안 용량을 계산할 수 있다. 보안 용량은 통신 효율에 관련된 지표로서, 양자직접통신을 통해 전송할 수 있는 데이터의 크기에 관한 정보를 의미할 수 있다.

[0027] 메모리(110)는 전자 장치(100) 내에서 처리되는 각종 데이터들을 저장하는 하드웨어로서, 메모리(110)는 전자 장치(100)에서 처리된 데이터들 및 처리될 데이터들을 저장할 수 있다. 또한, 메모리(110)는 전자 장치(100)에 의해 구동될 애플리케이션들, 드라이버들 등을 저장할 수 있다. 메모리(110)는 DRAM(dynamic random access memory), SRAM(static random access memory) 등과 같은 RAM(random access memory), ROM(read-only memory), EEPROM(electrically erasable programmable read-only memory), CD-ROM, 블루레이 또는 다른 광학 디스크 스토리지, HDD(hard disk drive), SSD(solid state drive), 또는 플래시 메모리를 포함할 수 있다.

[0028] 프로세서(120)는 전자 장치(100)의 전반적인 기능들을 제어하는 역할을 한다. 예를 들어, 프로세서(120)는 전자 장치(100) 내의 메모리(110)에 저장된 프로그램들을 실행함으로써, 전자 장치(100)를 전반적으로 제어한다. 프로세서(120)는 전자 장치(100) 내에 구비된 CPU(central processing unit), GPU(graphics processing unit), AP(application processor) 등으로 구현될 수 있으나, 이에 제한되지 않는다.

[0029] 일 실시예에 따라, 프로세서(120)는 양자직접통신에 관한 시뮬레이션을 수행할 수 있다. 구체적으로, 프로세서(120)는 양자직접통신을 위한 프로토콜에 따른 도청에 의해 간섭 받는 양자직접통신에 관한 시뮬레이션을 수행할 수 있다. 다른 실시예에 따라, 프로세서(120)는 외부 장치로부터 양자직접통신에 관한 실험 데이터를 획득할 수 있다. 일 실시예에 따라, 양자직접통신을 위한 프로토콜은 DL04 프로토콜을 포함할 수 있으나 이에 제한되지 않는다.

[0031] 도 2a는 일 실시예에 따른 시뮬레이션의 실제 모델인 양자직접통신 실험의 구성도를 나타낸다.

[0032] 양자직접통신은 양자 채널의 상황을 파악하여 전송하고자 하는 메시지를 직접적으로 암호화한 후에 전송하는 통신 방법이다. 도 2a를 참조하면, 양자직접통신은 수신 장치(200)와 송신 장치(210) 간에 이루어질 수 있다. 도청 장치(220)는 수신 장치(200)와 송신 장치(210)간의 양자직접통신에 간섭할 수 있다. 도 2a를 참조하면, 수신 장치(200)는 Det(Detector), LS(Laser Source), CIR(Circulator), BS(Beam Splitter), PM(Phase Modulator), 및 PBS(Polarized Beam Splitter)를 포함할 수 있다. Det는 광자를 검출할 수 있고, LS는 광자를 포함하는 레이저 펄스를 생성할 수 있고, CIR은 레이저 펄스가 단방향으로 진행하도록 설정할 수 있고, BS는 레이저 펄스를 적어도 2개 이상으로 분할할 수 있고, PM은 레이저 펄스의 위상을 변조할 수 있고, PBS는 하나의 편광 상태의 레이저 펄스를 반사시키고 직교 상태의 레이저 펄스를 투과시킬 수 있다. 예를 들어, CIR은 LS로부터 생성된 레이저 펄스가 BS로 Det로 전달되지 않고 BS로 전달되도록 방향을 설정할 수 있다. QC는 양자 채널(Quantum Channel)을 의미할 수 있다. 송신 장치(210)는 Det(Detector), BS(Beam Splitter), PBS(Polarized Beam Splitter), FR(Faraday Rotator), 및 PM(Phase Modulator)을 포함할 수 있다. FR은 편광을 45도 회전시킬 수 있다. DL은 지연선(Delay Line)을 의미할 수 있고, 기 설정된 시간 동안 광섬유(Optical Fiber)에 레이저 펄스를 잔류시킴으로써 양자 메모리(Quantum Memory)의 역할을 수행할 수 있다. 송신 장치(210)는 위상 인코딩부(211)와 간섭계부(212)로 구성될 수 있다. 위상 인코딩부(211)와 간섭계부(212)에 관한 설명은 이하 도 2b에서 상세히 설명될 것이다.

[0033] 도 2a를 통한 양자직접통신의 전체적인 흐름은 다음과 같다. 양자직접통신을 위한 준비(Preparation) 단계에서, 수신 장치(200)의 LS는 단일 광자열을 생성할 수 있다. 각 광자들은 $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ 중 하나의 상태(state)를 가질 수 있다. 여기서, $|0\rangle, |1\rangle$ 는 Z 기저의 고유벡터(eigenvector)를 의미할 수 있고, $|+\rangle, |-\rangle$ 는 X 기저의 고유벡터를 의미할 수 있다. 수신 장치(200)는 PM을 이용하여 광자의 위상을 4가지로 변조하여 전송할 수 있다. 예를 들어, 수신 장치(200)는 PM을 이용하여 광자의 위상을 $0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}$ 로 변조(또는, 인코딩)할 수 있다. 수신 장치(200)는 변조된 광자를 양자 채널(QC)을 통해 송신 장치(210)로 전송할 수 있다.

[0034] 양자직접통신을 위한 에러 체크(Error Check) 단계에서, 송신 장치(210)는 양자 채널 환경을 파악하기 위해, 수신 장치(200)로부터 전송받은 단일 광자열 중 적어도 일부를 무작위로 추출하여 측정할 수 있다. 수신 장치(200)는 측정 시에 X 기저 또는 Z 기저를 이용할 수 있다. 다시 말해, 수신 장치(200)는 PM을 통해 0으로 디코딩하거나, $\frac{\pi}{2}$ 로 디코딩할 수 있다. 송신 장치(210)는 측정 시에 이용한 기저(X 기저 또는 Z 기저), 측정 결과를 수신 장치(200)에게 공개할 수 있다. 수신 장치(200)는 송신 장치(210)가 공개한 결과를 기초로 수신 장치(200)와 송신 장치(210) 간의 DBER(Detection Bit Error Rate)을 연산하여 송신 장치(210)에게 전송할 수 있다. DBER이 기 설정된 허용 오류율 이하인 경우, 양자 채널 환경이 양자직접통신에 적합하다고 판단할 수 있다.

[0035] 양자직접통신을 위한 인코딩 단계에서, 송신 장치(210)는 정보 인코딩(Information Encoding)을 수행할 수 있다. 송신 장치(210)는 0비트(bit)를 전송하고자 하는 경우, $I = |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ 를 이용하여 인코딩을 수행하고, 1비트를 전송하고자 하는 경우, $Y = |0\rangle\langle 1| - |1\rangle\langle 0| = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ 를 이용하여 인코딩을 수행할 수 있다. 송신 장치(210)는 도청 장치(220)의 접근을 방지하기 위해, 별도의 체크 비트(Check Bit)를 임의로 부가하여 전송할 수 있다. 예를 들어, 송신 장치(210)가 110011의 정보 비트를 수신 장치(200)로 전송하는 경우, 송신 장치(210)는 000의 체크 비트를 부가하여, 총 110011000의 비트를 수신 장치(200)로 전송할 수 있다.

[0036] 양자직접통신을 위한 디코딩 단계에서, 수신 장치(200)는 준비 단계에서 사용한 기저(X기저 또는 Z기저)를 이용

하여 송신 장치(210)로부터 전송 받은 비트를 디코딩할 수 있다. 디코딩 단계는 양자 채널 환경을 측정하기 위해, 에러 체크 단계에서 DBER을 측정하는 것과 마찬가지로 수신 장치(200)와 송신 장치(210) 간의 QBER(Quantum Bit Error Rate)을 연산할 수 있다. QBER이 기 설정된 허용 오류율을 초과하는 경우, 수신 장치(200)는 양자직접통신을 중단할 수 있다.

[0037] 양자직접통신의 실험을 위해서는 수신 장치(200)와 송신 장치(210)의 LS가 단일광자열을 직접 생성하여 전송하는 것이 가장 이상적이지만, 기술적 한계로 인해 LS는 일반적인 레이저 펄스를 감쇄하여 사용할 수 있다. 일반적인 레이저 펄스를 감쇄하여 사용하는 경우, 일정 확률로 단일광자가 아닌 다중광자가 존재할 확률이 존재할 수 있다. 다중광자가 존재하는 경우, 도청 장치(220)는 다중광자 중 적어도 일부의 단일광자를 포획할 수 있다. 도청 장치(220)의 포획 과정은 다른 광자에 영향을 주지 않으면서 수신 장치(200) 및 송신 장치(210)와 동일한 정보를 획득할 수 있다. 이를 방지하기 위해, 신호 상태(signal state)와 더불어 미끼 상태(decoy state)를 도입하여 실험을 수행할 수 있다.

[0039] 도 2b는 일 실시예에 따른 위상 인코딩부(211) 및 간섭계부(212) 간의 관계를 나타낸다.

[0040] 도 2b를 참조하면, 송신 장치(210)는 전송할 광자를 인코딩하는 위상 인코딩부(211) 및 수신 장치(200)로부터 전송 받은 광자를 이용하여 채널 환경을 파악하는 간섭계부(212)를 포함할 수 있다. 도청 장치(220)가 포획하는 정보량을 최소화하기 위해서는 송신 장치(210)가 측정하는 광자 비율(γ^A)에 대한 도청 장치(220)가 측정하는 광자 비율(γ^E)이 1이 되어야 한다. 일 실시예에 따라, 송신 장치(210)의 Det 효율은 70%일 수 있고, 도청 장치(220)의 Det 효율은 100%일 수 있다. 일 실시예에 따라, 인코딩부(211)의 감쇄율은 $10^{-4.6/10}$일 수 있고, 간섭계부(212)의 감쇄율은 $10^{-2.3/10}$ 일 수 있다. 상기 송신 장치(210) 및 도청 장치(220)의 Det 효율, 및 인코딩부(211) 및 간섭계부(212)의 감쇄율에 따른 송신 장치(210) 및 도청 장치(220)가 측정하는 광자 비율(γ^A, γ^E)은 아래 수학식 1을 통해 계산될 수 있다.

[0041] [수학식 1]

$$\gamma^A = (1-k)\cdot 10^{-\frac{2.3}{10}}\cdot 0.7$$

[0042] $$\gamma^E = k^2\cdot 10^{-\frac{4.6}{10}}\cdot 1$$

[0043] 수학식 1을 참조하면, γ^A는 송신 장치(210)가 측정하는 광자 비율을 의미할 수 있고, γ^E는 도청 장치(220)가 측정하는 광자 비율을 의미할 수 있고, k는 인코딩부(211) 및 간섭계부(212) 간의 BS의 Beam Splitting Ratio를 의미할 수 있다. 도 2b를 참조하면, 양자 채널을 통과한 광자는 BS를 기점으로 k만큼 인코딩부(211)로 전달되고, $1-k$ 만큼 간섭계부(212)로 전달될 수 있다. 전술한 바와 같이, 도청 장치(220)가 포획하는 정보량을 최소화하기 위해서는 $\frac{\gamma^E}{\gamma^A}=1$ 이 되어야 하므로, 인코딩부(211) 및 간섭계부(212) 간의 BS의 Beam Splitting Ratio k는 0.6573으로 시뮬레이션이 수행될 수 있다.

[0044] 다시 도 1을 참조하면, 일 실시예에 따라 프로세서(120)는 제1정보, 제2정보, 및 에러율에 관한 정보를 확인할 수 있다. 제1정보는 평균 광자수(Mean Photon Number)가 제1값인 신호 상태(signal state)일 때 수신 장치가 생성한 레이저 펄스에 포함되는 제1광자가 제1경로를 통해 수신 장치에서 검출되는 확률에 관한 정보를 포함할 수 있다. 여기서, 신호 상태는 평균 광자수가 μ인 경우를 의미할 수 있고, 제1경로는 제1광자가 수신 장치로부터 송신 장치를 거쳐 수신 장치로 전송되는 경로를 포함할 수 있다. 제2정보는 제1광자가 제2경로를 통해 도청 장치에서 검출되는 확률에 관한 정보를 포함할 수 있다. 여기서, 제2경로는 제1광자가 수신 장치로부터 송신 장치를 거쳐 도청 장치로 전송되는 경로를 포함할 수 있다. 에러율에 관한 정보는 구체적으로, DBER에 관한 정보의 제1상한, 및 QBER에 관한 정보를 포함할 수 있다. 프로세서(120)는 제1정보, 제2정보, 및 에러율에 관한 정보를 확인하고 아래 수학식 2를 통해 양자직접통신을 위한 프로토콜의 보안 용량을 계산할 수 있다.

[0045] [수학식 2]

[0046] $$C_s = Q_\mu^{BAB}\left[1 - h\left(E_\mu^{BAB}\right)\right] - Q_{\mu,n=1}^{BAE} h\left(2e_1^{BA,U}\right) - Q_{\mu,n=2}^{BAE} \cdot \left(\frac{1}{2} h\left(2e_2^{BA,U}\right) + \frac{1}{2}\right) - Q_{\mu,n\geq 3}^{BAE} \cdot 1$$

[0047] 수학식 2를 참조하면, C_s은 프로토콜의 보안 용량을 의미할 수 있고, Q_μ^{BAB}는 제1정보를 의미할 수 있고, h는 샤논 엔트로피(Shannon Entropy)를 의미할 수 있고, $Q_{\mu,n=1}^{BAE}$, $Q_{\mu,n=2}^{BAE}$, $Q_{\mu,n\geq 3}^{BAE}$ 는 제2정보를 의미할 수 있고, E_μ^{BAB}, e_1^{BA}, e_2^{BA}는 에러율에 관한 정보(또는, E_μ^{BAB}는 QBER에 관한 정보, $e_1^{BA,U}$, $e_2^{BA,U}$는 DBER에 관한 정보의 제1상한으로 지칭됨)를 의미할 수 있다. 제1정보(Q_μ^{BAB})의 아랫첨자는 평균광자수가 μ인 신호 상태를 의미하고, 윗첨자(BAB)는 광자가 밥(수신 장치)으로부터 엘리스(송신 장치)를 거쳐 다시 밥(수신 장치)로 전송되는 제1경로를 의미하므로, 결국 제1정보(Q_μ^{BAB})는 신호 상태일 때 수신 장치가 생성한 레이저 펄스에 포함되는 제1광자가 제1경로를 통해 수신 장치에서 검출되는 확률에 관한 정보를 의미할 수 있다. 마찬가지로, 제2정보(E_μ^{BAB})는 제1광자가 제1경로를 통해 전송될 때의 QBER에 관한 정보를 의미할 수 있다.

[0048] 일 실시예에 따라, 제2정보는 제2-1정보, 제2-2정보, 및 제2-3정보를 포함할 수 있다. 구체적으로, 제2-1정보는 제2경로를 통해 도청 장치에서 제1광자가 제1개수 검출되는 확률에 관한 정보를 포함할 수 있고, 제2-2정보는 제2경로를 통해 도청 장치에서 제1광자가 제2개수 검출되는 확률에 관한 정보를 포함할 수 있고, 제2-3정보는 제2경로를 통해 도청 장치에서 제1광자가 적어도 제3개수 검출되는 확률에 관한 정보를 포함할 수 있다. 수학식 2를 참조하면, 제2정보($Q_{\mu,n=1}^{BAE}$, $Q_{\mu,n=2}^{BAE}$, $Q_{\mu,n\geq 3}^{BAE}$)의 윗첨자(BAE)는 제2경로를 통해 전송된다는 것을 의미하고, 제2정보의 아랫첨자($\mu, n=1,\ \mu, n=2, \mu, n\geq 3$)는 제1광자가 검출되는 개수를 의미할 수 있다. 일 실시예에 따라, 제1개수는 1개를 포함할 수 있고, 제2개수는 2개를 포함할 수 있고, 제3개수는 3개를 포함할 수 있으나, 제1개수, 제2개수, 및 제3개수는 이에 제한되지 않고 보안 용량을 계산하기 위해 필요한 적절한 개수가 이용될 수 있다. 제2-1정보, 제2-2정보, 및 제2-3정보는 아래 수학식 3을 통해 계산될 수 있다.

[0049] [수학식 3]

[0050] $$Q_{\mu,n=1}^{BAE} = p(1,\mu)Y_1^{A,L} - p(1,\mu)Y_0^A$$

$$Q_{\mu,n=2}^{BAE} = p(2,\mu)Y_2^{A,L} - p(2,\mu)Y_0^A$$

$$Q_{\mu,n\geq 3}^{BAE} = 1 - Q_{\mu,n=1}^{BAE} - Q_{\mu,n=2}^{BAE}$$

$$p(n,\mu) = \frac{\mu^n}{n!}e^{-\mu}$$

[0051] 수학식 3을 참조하면, $Q_{\mu,n=1}^{BAE}$는 제2-1정보를 의미할 수 있고, $Q_{\mu,n=2}^{BAE}$는 제2-2정보를 의미할 수 있고, $Q_{\mu,n\geq 3}^{BAE}$는 제2-3정보를 의미할 수 있고, $p(1,\mu)$는 제1포아송 정보를 의미할 수 있고, $p(2,\mu)$는 제2포아송 정보를 의미할 수 있고, $Y_1^{A,L}$는 제1산출 정보의 제1하한을 의미할 수 있고, $Y_2^{A,L}$는 제2산출 정보의 제1하한을 의미할 수 있고, Y_0^A는 제3산출 정보를 의미할 수 있다.

[0052] 수학식 3을 참조하면, 제2-1정보($Q_{\mu,n=1}^{BAE}$)는 제1포아송 정보($p(1,\mu)$), 제1산출 정보의 제1하한($Y_1^{A,L}$), 및 제3산출 정보(Y_0^A)를 기초로 계산될 수 있다. 제1포아송 정보는, 평균광자수가 μ인 신호 상태일 때 수신 장치가 생성할 레이저 펄스에 제1광자가 제1개수 포함될 학률에 관한 정보를 포함할 수 있다. 제1개수는 1개를 포함할 수 있으나, 이에 제한되지 않는다. 결국 제1포아송 정보는 $p(1,\mu) = \frac{\mu^1}{1}e^{-\mu} = \mu \cdot e^{-\mu}$ 을 의미할 수 있고, e는 자연 로그를 의미할 수 있다. 제1산출 정보는 수신 장치에서 제1개수의 제1광자가 생성되어 송신 장치로 전송된 경우 송신 장치에서 제1광자가 검출되는 확률에 관한 정보를 포함할 수 있다. 제3산출 정보는 수신 장치에서 제1광자가 생성되지 않았음에도 송신 장치에서 제1광자가 검출된 것으로 판단한 확률에 관한 정보를 포함할 수 있다.

[0053] 수학식 3을 참조하면, 제2-2정보($Q_{\mu,n=2}^{BAE}$)는 제2포아송 정보($p(2,\mu)$), 제2산출 정보의 제1하한($Y_2^{A,L}$), 및 제3산출 정보(Y_0^A)를 기초로 계산될 수 있다. 제2포아송 정보는 평균광자수가 μ인 신호 상태일 때 수신 장치가 생성할 레이저 펄스에 제1광자가 제2개수 포함될 확률에 관한 정보를 포함할 수 있다. 제2개수는 2개를 포함할 수 있으나, 이에 제한되지 않는다. 제2산출 정보는 수신 장치에서 제2개수의 제1광자가 생성되어 송신 장치로 전송된 경우 송신 장치에서 제1광자가 검출되는 확률에 관한 정보를 포함할 수 있다.

[0054] 수학식 3을 참조하면, 제2-3정보($Q_{\mu,n\geq 3}^{BAE}$)는 제2-1정보($Q_{\mu,n=1}^{BAE}$) 및 제2-2정보($Q_{\mu,n=2}^{BAE}$)를 기초로 계산될 수 있다. 결과적으로, 제2-1정보($Q_{\mu,n=1}^{BAE}$), 제2-2정보($Q_{\mu,n=2}^{BAE}$), 및 제2-3정보($Q_{\mu,n\geq 3}^{BAE}$)는 제1산출 정보의 제1하한($Y_1^{A,L}$), 제2산출 정보($Y_2^{A,L}$)의 제1하한을 기초로 계산될 수 있다. 제1산출 정보의 제1하한, 제2산출 정보의 제1하한은 아래 수학식 4를 통해 계산될 수 있다.

[0055] [수학식 4]

$$Y_1^{A,L} = \frac{\mu^2\left(Q_{\nu_2}^{BA}e^{\nu_2} - Q_{\nu_3}^{BA}e^{\nu_3}\right) - (\nu_2^2 - \nu_3^2)(Q_\mu^{BA}e^{\mu} - Y_0^A)}{\mu(\nu_2 - \nu_3)(\mu - \nu_2 - \nu_3)}$$

$$Y_2^{A,L} = \frac{2\mu\left(Q_{\nu_1}^{BA}e^{\nu_1} - Q_{\nu_2}^{BA}e^{\nu_2}\right) - 2(\nu_1 - \nu_2)(Q_\mu^{BA}e^{\mu} - Y_0^A)}{\mu(\nu_1 - \nu_2)(\nu_1 + \nu_2 - \mu)}$$

[0056]

[0057] 수학식 4를 참조하면, $Y_1^{A,L}$는 제1산출 정보의 제1하한을 의미할 수 있고, $Y_2^{A,L}$는 제2산출 정보의 제1하한을 의미할 수 있고, Y_0^A는 제3산출 정보를 의미할 수 있고, e는 자연로그를 의미할 수 있고, μ는 신호 상태의 평균광자수를 의미할 수 있고, ν_1는 제1미끼 상태일 때의 평균 광자수를 의미할 수 있고, ν_2는 제2미끼 상태일 때의 평균광자수를 의미할 수 있고, ν_3는 제3미끼 상태일 때의 평균광자수를 의미할 수 있고, $Q_{\nu_1}^{BA}$는 제3-1정보를 의미할 수 있고, $Q_{\nu_2}^{BA}$는 제3-2정보를 의미할 수 있고, $Q_{\nu_3}^{BA}$는 제3-3정보를 의미할 수 있고, Q_μ^{BA}는 제4정보를 의미할 수 있다. 제3-1정보($Q_{\nu_1}^{BA}$)는 평균광자수가 제2-1값인 제1미끼 상태일 때 수신 장치가 생성한 레이저 펄스에 포함되는 제2-1광자가 제3경로를 통해 수신 장치에서 검출되는 확률에 관한 정보를 포함할 수 있다. 여기서 제3경로는, 광자가 밥(수신 장치)으로부터 이브(도청 장치)를 거치지 않고 엘리스(송신 장치)로 전송되는 경로(BA)를 포함할 수 있다. 예를 들어, 제3-1정보($Q_{\nu_1}^{BA}$)는 평균광자수가 ν_1인 제1미끼 상태일 때 수신 장치가 생성한 레이저 펄스에 포함되는 제2-1광자가 BA 경로를 통해 수신 장치에서 검출되는 확률에 관한 정보를 포함할 수 있다. 제3-2정보($Q_{\nu_2}^{BA}$)는 평균광자수가 제2-2값인 제2미끼 상태일 때 수신 장치가 생성한 레이저 펄스에 포함되는 제2-2광자가 제3경로를 통해 수신 장치에서 검출되는 확률에 관한 정보를 포함할 수 있다. 예를 들어, 제3-2정보($Q_{\nu_2}^{BA}$)는 평균광자수가 ν_2인 제2미끼 상태일 때 수신 장치가 생성한 레이저 펄스에 포함되는 제2-2광자가 BA 경로를 통해 수신 장치에서 검출되는 확률에 관한 정보를 포함할 수 있다. 제3-3정보($Q_{\nu_3}^{BA}$)는 평균광자수가 제2-3값인 제3미끼 상태일 때 수신 장치가 생성한 레이저 펄스에 포함되는 제2-3광자가 제3경로를 통해 수신 장치에서 검출되는 확률에 관한 정보를 포함할 수 있다. 예를 들어, 제3-3정보($Q_{\nu_3}^{BA}$)는 평균광자수가 ν_3인 제3미끼 상태일 때 수신 장치가 생성한 레이저 펄스에 포함되는 제2-3광자가 BA 경로를 통해 수신 장치에서 검출되는 확률에 관한 정보를 포함할 수 있다. 제4정보(Q_μ^{BA})는 제1광자가 제3경로를 통해 수신 장치에서 검출되는 확률에 관한 정보를 포함할 수 있다. 예를 들어, 제4정보(Q_μ^{BA})는 평균광자수가 μ인 신호 상태일 때 수신 장치가 생성한 레이저 펄스에 포함되는 제1광자가 BA경로를 통해 수신 장치에서 검출되는 확률에 관한 정보를 포함할 수 있다.

[0058] 일 실시예에 따라, 제1산출 정보의 제1하한($Y_1^{A,L}$)은 제1값, 제2-2값, 제2-3값, 제3-2정보, 제3-3정보, 제4정보, 및 제3산출 정보를 기초로 계산될 수 있다. 수학식 4를 참조하면, 제1산출 정보의 제1하한($Y_1^{A,L}$)은 제1값(μ), 제2-2값(ν_2), 제2-3값(ν_3), 제3-2정보($Q_{\nu_2}^{BA}$), 제3-3정보($Q_{\nu_3}^{BA}$), 제4정보(Q_μ^{BA}), 및 제3산출 정보(Y_0^A)를 기초로

계산될 수 있다. 일 실시예에 따라, 제3산출 정보(Y_0^A)는 시뮬레이션에서의 수신 장치 및 송신 장치의 기 설정된 다크 카운트율(Dark Count Rate)일 수 있다. 예를 들어, 제3산출 정보(Y_0^A)는 8×10^{-8} $per\ pulse$일 수 있다. 일 실시예에 따라, 제2산출 정보의 제1하한($Y_2^{A,L}$)은 제1값, 제2-1값, 제2-2값, 제3-1정보, 제3-2정보, 제4정보, 및 제3산출 정보를 기초로 계산될 수 있다. 수학식 4를 참조하면, 제2산출 정보의 제1하한($Y_2^{A,L}$)은 제1값(μ), 제2-1값(ν_1), 제2-2값(ν_2), 제3-1정보($Q_{\nu_1}^{BA}$), 제3-2정보($Q_{\nu_2}^{BA}$), 제4정보(Q_{μ}^{BA}), 및 제3산출 정보(Y_0^A)를 기초로 계산될 수 있다. 다시 수학식 2를 참조하면, 보안 용량은 에러율에 관한 정보를 기초로 계산될 수 있다. 일 실시예에 따라, 에러율에 관한 정보는, DBER에 관한 정보의 제1상한 및 QBER에 관한 정보를 포함할 수 있다. DBER에 관한 정보의 제1상한은 제1DBER에 관한 정보의 제1상한 및 제2DBER에 관한 정보의 제1상한을 포함할 수 있다. QBER에 관한 정보, 제1DBER에 관한 정보의 제1상한, 및 제2DBER에 관한 정보의 제1상한은 아래 수학식 5를 통해 계산될 수 있다.

[0059] [수학식 5]

$$E_{\mu}^{BAB} = \frac{e_0 Y_0^A + e_{det}^{BAB}(1 - e^{-\eta^{BAB}\mu})}{Q_{\mu}^{BAB}}$$

$$e_1^{BA,U} = \frac{E_{\nu_3}^{BA} Q_{\nu_3}^{BA} e^{\nu_3} - e_0 Y_0^A}{Y_1^{A,L} \nu_3}$$

$$e_2^{BA,U} = \frac{2(E_{\nu_2}^{BA} Q_{\nu_2}^{BA} e^{\nu_2} - \frac{\nu_2}{\nu_3} E_{\nu_3}^{BA} Q_{\nu_3}^{BA} e^{\nu_3} + \frac{\nu_2 - \nu_3}{\nu_3} e_0 Y_0^A)}{Y_2^{A,L} \nu_2 (\nu_2 - \nu_3)}$$

$$E_{\alpha}^{BA} = \frac{e_0 Y_0^A + e_{det}^{BA}(1 - e^{-\eta^{BA}\alpha})}{Q_{\alpha}^{BA}}, \quad \alpha \in \{\nu_2, \nu_3\}$$

[0060]

[0061] 수학식 5를 참조하면, E_{μ}^{BAB}는 QBER에 관한 정보를 의미할 수 있고, $e_1^{BA,U}$는 제1DBER에 관한 정보의 제1상한을 의미할 수 있고, $e_2^{BA,U}$는 제2DBER에 관한 정보의 제1상한을 의미할 수 있다. 수학식 5를 참조하면, QBER에 관한 정보(E_{μ}^{BAB})는 수신 장치의 검출 에러(e_{det}^{BAB}), 제1경로로 전송되는 과정에서 발생하는 감쇄율(η^{BAB}), 제3산출 정보(Y_0^A), 및 e_0를 기초로 계산될 수 있다. 수신 장치의 검출 에러(e_{det}^{BAB}), 제1경로로 전송되는 과정에서 발생하는 감쇄율(η^{BAB}), 제3산출 정보(Y_0^A), 및 e_0는 기 설정될 수 있다. 예를 들어, 수신 장치의 검출 에러(e_{det}^{BAB})는 0.26%일 수 있고, 제3산출 정보(Y_0^A)는 8×10^{-8} $per\ pulse$일 수 있고, e_0는 $\frac{1}{2}$ 일 수 있다. 일 실시예에 따라, 제1DBER에 관한 정보의 제1상한은 제1산출 정보, 제2-3값, 제2-3광자를 제3경로를 통해 전송할 경우의 BER(Bit Error Rate)에 관한 정보, 제3-3정보, 및 제3산출 정보를 기초로 계산될 수 있다. 수학식 5를 참조하면, 제1DBER에 관한 정보의 제1상한($e_1^{BA,U}$)은 제1산출 정보의 제1하한($Y_1^{A,L}$), 제2-3값(ν_3), 제2-3광자를 제3경로를 통해 전송할 경우의 BER에 관한 정보($E_{\nu_3}^{BA}$), 제3-3정보($Q_{\nu_3}^{BA}$), 및 제3산출 정보(Y_0^A)를 기초로 계산될 수 있다. 일 실시예에 따라, 제2DBER에 관한 정보의 제1상한은 제2산출 정보의 제1하한, 제2-2값, 제2-3값, 제2-2광자를 제3경로를 통해 전송할 경우의 BER에 관한 정보, 제3-2정보, 제2-3광자를 제3경로를 통해 전송할 경우의 BER에 관한 정보, 제3-3정보, 및 제3산출 정보를 기초로 계산될 수 있다. 수학식 5를 참조하면, 제2DBER에 관한 정보의 제1상한($e_2^{BA,U}$)은 제2산출 정보의 제1하한($Y_2^{A,L}$), 제2-2값(ν_2), 제2-3값(ν_3), 제2-2광자를 제3경로를 통해 전송할 경우의 BER에 관한 정보($E_{\nu_2}^{BA}$), 제3-2정보($Q_{\nu_2}^{BA}$), 제2-3광자를 제3경로를 통해 전송할 경우의 BER에 관한 정보($E_{\nu_3}^{BA}$), 제3-3정보($Q_{\nu_3}^{BA}$), 및 제3산출 정보(Y_0^A)를 기초로 계산될 수 있다. 수학식 5를 참조하면, 제2-2광자를 제3경로를 통해 전송할 경우의 BER에 관한 정보($E_{\nu_2}^{BA}$)는 제3산출 정보(Y_0^A), 제3-2정보($Q_{\nu_2}^{BA}$), 제3경로로 전송되는 과정에서 발생하는 감쇄율(η^{BA}), 송신 장치의 검출 에러(e_{det}^{BA})를 기초로 계산될 수 있고, 제2-3광자를 제3경로를 통해 전송할 경우의 BER에 관한 정보($E_{\nu_3}^{BA}$)는 제3산출 정보(Y_0^A), 제3-3정보

($Q_{\nu_x}^{BA}$), 제3경로로 전송되는 과정에서 발생하는 감쇄율(η^{BA}), 송신 장치의 검출 에러(e_{det}^{BA})를 기초로 계산될 수 있다. 일 실시예에 따라, 제3경로로 전송되는 과정에서 발생하는 감쇄율(η^{BA}), 송신 장치의 검출 에러(e_{det}^{BA})는 기 설정될 수 있다. 예를 들어, 송신 장치의 검출 에러(e_{det}^{BA})는 1.31%일 수 있다.

[0062] 다시 도 1을 참조하면, 일 실시예에 따라 프로세서(120)는 가우시안 근사를 이용하여 제1정보, 제2정보, 및 에러율에 관한 정보의 상한 및 하한 중 적어도 하나를 계산할 수 있다. 가우시안 근사 방법은 대표적인 통계적 분석 방법이다. $\alpha \in \{\mu, \nu_1, \nu_2, \nu_3, \nu_4\}$ 평균광자수를 사용했을 때 검출되는 사건의 수를 M_α라고 가정하고, N_α를 α 평균광자수를 사용하는 데이터 사이즈라고 가정하면, Q_α($Q_\alpha = \frac{M_\alpha}{N_\alpha}$)는 α 평균광자수를 사용했을 때 광자가 이론적으로 검출될 확률일 수 있다. 이 때 M_α는 $M_\alpha \sim B(N_\alpha, Q_\alpha)$의 이항분포를 따를 수 있다. N_α가 충분히 크다고 가정하면, M_α는 $M_\alpha \sim N(N_\alpha Q_\alpha, N_\alpha Q_\alpha(1-Q_\alpha))$로 정규분포를 따를 수 있다. $Q_\alpha = \frac{M_\alpha}{N_\alpha}$므로, Q_α도 $Q_\alpha \sim N(Q_\alpha, \frac{Q_\alpha(1-Q_\alpha)}{N_\alpha})$의 정규분포를 따를 수 있다. 일 실시예에 따라 프로세서(120)는 기 설정된 추정 실패 확률(Failure Probability) 및 표준 정규 분포(Standard Normal Distribution)의 역누적분포함수(Inverse Cumulative Distribution Function)에 기초하여 신뢰도를 계산하고, 신뢰도에 기초하여 제1정보, 제2정보, 및 에러율에 관한 정보의 상한 및 하한 중 적어도 하나를 계산할 수 있다. Q_α가 정규분포를 만족하므로 추정 실패 확률을 ε이라고 가정하면, $\Pr[E[Q_\alpha] - Q_\alpha \geq \varphi\sqrt{\frac{Q_\alpha(1-Q_\alpha)}{N_\alpha}}] \leq \varepsilon$을 만족할 수 있다. 일 실시예에 따라 추정 실패 확률(ε)은 10^{-10}로 기 설정될 수 있다. 여기서 φ는 신뢰도로서, 표준 정규 분포의 역누적분포함수에 따라 $\varphi = \Phi^{-1}(1-\frac{\varepsilon}{2})$으로 계산될 수 있다. Q_α의 상한과 하한은 아래 수학식 6을 통해 계산될 수 있다.

[0063] [수학식 6]

[0064] $$E^U[Q_\alpha] = Q_\alpha + \varphi\sqrt{\frac{Q_\alpha(1-Q_\alpha)}{N_\alpha}}$$

[0065] $$E^L[Q_\alpha] = Q_\alpha - \varphi\sqrt{\frac{Q_\alpha(1-Q_\alpha)}{N_\alpha}}$$

[0066] 수학식 6을 참조하면, $E^U[Q_\alpha]$는 Q_α의 상한을 의미할 수 있고, $E^L[Q_\alpha]$는 Q_α의 하한을 의미할 수 있고, Q_α($Q_\alpha = \frac{M_\alpha}{N_\alpha}$)는 α 평균광자수를 사용했을 때 광자가 이론적으로 검출될 확률을 의미할 수 있고, φ는 신뢰도를 의미할 수 있고, N_α를 α 평균광자수를 사용하는 데이터 사이즈를 의미할 수 있다. 수학식 6의 방식을 통해 Q_α의 상한과 하한을 계산하는 방법을 수학식 2에 적용하면 아래 수학식 7과 같을 수 있다.

[0067] [수학식 7]

[0068] $$C_s = E^L[Q_\mu^{BAB}]\left[1 - h\left(E^U\left(E_\mu^{BAB}\right)\right)\right] - E^L[Q_{\mu,n=1}^{BAE}]h\left(2E^U\left[e_1^{BA,U}\right]\right) - E^L[Q_{\mu,n=2}^{BAE}] \cdot \left(\frac{1}{2}h\left(2E^U[e_2^{BA,U}]\right) + \frac{1}{2}\right) - E^U[Q_{\mu,n\geq 3}^{BAE}] \cdot 1$$

[0069] 본 개시는 수학식 6과 같은 가우시안 근사 방식을 통해 각 정보의 상한과 하한을 설정하여 보다 현실에 적합한 보안 용량을 확인할 수 있다. 다시 말해, 본 개시는 무한한 데이터 사이즈를 가정하고 보안 용량을 계산하는 종래 방법과 달리, 가우시안 근사를 이용하여 보안 용량을 계산함으로써 유한한 데이터 사이즈를 사용할 때 발생하는 통계적 변동을 고려한 보안 용량 계산이 가능할 수 있다. 일 실시예에 따라, 프로세서(120)는 제1정보, 제2정보, 및 에러율에 관한 정보의 상한 및 하한 중 적어도 하나에 기초하여 보안 용량을 계산할 수 있다. 구체적

으로, 프로세서(120)는 제1정보의 하한, QBER에 관한 정보의 상한, 제2-1정보의 하한, 제2-2정보의 하한, 제2-3정보의 상한, 및 DBER에 관한 정보의 제2상한에 기초하여 보안 용량을 계산할 수 있다. 예를 들어, 수학식 7을 참조하면 보안 용량(C_s)은 제1정보의 하한($E^L[Q_\mu^{BAB}]$), QBER에 관한 정보의 상한($E^U(E_\mu^{BAB})$), 제2-1정보의 하한($E^L[Q_{\mu,n=1}^{BAE}]$), 제2-2정보의 하한($E^L[Q_{\mu,n=2}^{BAE}]$), 제2-3정보의 상한($E^U[Q_{\mu,n\geq 3}^{BAE}]$), 및 DBER에 관한 정보의 제2상한($E^U[e_1^{BA,U}]$, $E^U[e_2^{BA,U}]$)에 기초하여 계산될 수 있다. 일 실시예에 따라, DBER에 관한 정보의 제2상한($E^U[e_1^{BA,U}]$, $E^U[e_2^{BA,U}]$)은, DBER에 관한 제1상한($e_1^{BA,U}$, $e_2^{BA,U}$)을 기초로 수학식 6의 방식을 이용하여 계산될 수 있다. 수학식 7과 마찬가지로, 수학식 6의 방식을 통해 제1산출 정보의 제2하한, 제2산출 정보의 제2하한, 제1DBER에 관한 정보의 제2상한, 및 제2DBER에 관한 정보의 제2을 계산할 수 있다. 예를 들어, 수학식 6의 방식을 통해 제1산출 정보의 제2하한을 아래 수학식 8과 같이 계산할 수 있다.

[0070] [수학식 8]

[0071]
$$E^L[Y_1^{A,L}] = \frac{\mu^2\left(E^L[Q_{\nu_2}^{BA}]e^{\nu_2} - E^U[Q_{\nu_3}^{BA}]e^{\nu_3}\right) - (\nu_2^2 - \nu_3^2)(E^U[Q_\mu^{BA}]e^{\mu} - Y_0^A)}{\mu(\nu_2 - \nu_3)(\mu - \nu_2 - \nu_3)}$$

[0072] 일 실시예에 따라, 제2-1정보의 하한은 제1산출 정보의 제2하한을 기초로 계산될 수 있다. 제1산출 정보의 제2하한은 제1값, 제2-2값, 제2-3값, 제3-2정보의 하한, 제3-3정보의 상한, 제4정보의 상한, 및 제3산출 정보를 기초로 계산될 수 있다. 수학식 8을 참조하면, 제1산출 정보의 제2하한($E^L[Y_1^{A,L}]$)은 제1값(μ), 제2-2값(ν_2). 제2-3값(ν_3), 제3-2정보의 하한($E^L[Q_{\nu_n}^{BA}]$), 제3-3정보의 상한($E^U[Q_{\nu_n}^{BA}]$), 제4정보의 상한($E^U[Q_\mu^{BA}]$), 및 제3산출 정보(Y_0^A)를 기초로 계산될 수 있다. 일 실시예에 따라, 제2-2정보의 하한은 제2산출 정보의 제2하한을 기초로 계산될 수 있다. 제2산출 정보의 제2하한은 제1값, 제2-1값, 제2-2값, 제3-1정보의 하한, 제3-2정보의 상한, 제4정보의 상한, 및 제3산출 정보를 기초로 계산될 수 있다.

[0073] 일 실시예에 따라, 제1DBER에 관한 정보의 제2상한은 제1산출 정보의 제2하한, 제2-3값, 제2-3광자를 제3경로를 통해 전송할 경우의 BER에 관한 정보의 상한, 제3-3정보의 상한, 및 제3산출 정보를 기초로 계산될 수 있다. 일 실시예에 따라, 제2DBER에 관한 정보의 제2상한은 제2산출 정보의 제2하한, 제2-2값, 제2-3값, 제2-2광자를 제3경로를 통해 전송할 경우의 BER에 관한 정보의 상한, 제3-2정보의 상한, 제2-3광자를 제3경로를 통해 전송할 경우의 BER에 관한 정보의 하한, 제3-3정보의 하한, 및 제3산출 정보를 기초로 계산될 수 있다.

[0074] 일 실시예에 따라, 제1정보, 제3-1정보, 제3-2정보, 및 제3-3정보는 다른 복수의 파라미터들로 확인될 수 있다. 제1정보, 제3-1정보, 제3-2정보, 및 제3-3정보는 아래 수학식 9를 통해 확인될 수 있다.

[0075] [수학식 9]

[0076]
$$Q_\alpha^{BA\ or\ BAB} = \frac{\alpha\ 평균광자수를\ 갖는\ 상태에서\ Det에\ 의해\ 검출되는\ 광자\ 수}{P_\alpha N}, \quad \alpha \in \{\mu, \nu_1, \nu_2, \nu_3, \nu_4\}$$

[0077] 수학식 9를 참조하면, Q_μ^{BAB}는 제1정보를 의미할 수 있고, $Q_{\nu_1}^{BA}$는 제3-1정보를 의미할 수 있고, $Q_{\nu_n}^{BA}$는 제3-2정보를 의미할 수 있고, $Q_{\nu_n}^{BA}$는 제3-3정보를 의미할 수 있고, $Q_{\nu_4}^{BA}$는 평균광자수가 ν_4인 제4미끼 상태일 때 수신 장치가 생성한 레이저 펄스에 포함되는 제2-4광자가 BA 경로를 통해 수신 장치에서 검출되는 확률에 관한 정보인 제3-4정보를 의미할 수 있다. 일 실시예에 따라, 평균광자수 ν_4는 0개일 수 있다. 일 실시예에 따라, 복수의 파라미터들은 기 설정된 개수의 광자, 기 설정된 개수의 광자에 대한 제1광자의 개수의 비율, 기 설정된 개수의 광자에 대한 제2-1광자의 개수의 비율, 기 설정된 개수의 광자에 대한 제2-2광자의 개수의 비율, 기 설정된 개수의 광자에 대한 제2-3광자의 개수의 비율, 기 설정된 개수의 광자에 대한 평균 광자수가 제2-4값인 제4미끼 상태일 때 수신 장치가 생성한 레이저 펄스에 포함되는 제2-4광자의 개수의 비율, 제1값, 제2-1값, 제2-2값, 제2-3값, 및 제2-4값을 포함할 수 있다. 예를 들어, 복수의 파라미터들은 기 설정된 개수의 광자(N), N에 대한 제1광자의 개수의 비율(P_μ), N에 대한 제2-1광자의 개수의 비율(P_{ν_n}), N에 대한 제2-2광자의 개수의 비율(P_{ν_n}), N에 대한 제2-3광자의 개수의 비율(P_{ν_n}), N에 대한 제2-4광자의 개수의 비율(P_{ν_4}), 제1값(μ), 제2-1

값(ν_1), 제2-2값(ν_2), 제2-3값(ν_3), 및 제2-4값(ν_4)을 포함할 수 있다. 일 실시예에 따라, 프로세서(120)는 보안 용량이 최대가 되도록 하는 복수의 파라미터들을 확인할 수 있다. 구체적으로, 프로세서(120)는 기 설정된 제한 조건을 만족하면서 보안 용량이 최대가 되도록 하는 복수의 파라미터들을 확인하기 위해 양자직접통신에 관한 시뮬레이션을 수행할 수 있다. 기 설정된 제한 조건은 아래 수학식 10으로 나타낼 수 있다.

[0078] [수학식 10]

$$P_\mu + P_{\nu_1} + P_{\nu_2} + P_{\nu_3} + P_{\nu_4} = 1$$

$$0 < \nu_3 < \nu_2 \le \frac{2}{3}\mu < \nu_1 \le \frac{3}{4}\mu$$

$$\nu_1 + \nu_2 > \mu$$

$$\nu_2 + \nu_3 < \mu$$

$$\nu_1 - \nu_2 - \frac{\nu_1^3 - \nu_2^3}{\mu^2} = 0$$

[0079]

[0080] 수학식 10을 참조하면, P_μ는 기 설정된 개수의 광자(N)에 대한 제1광자의 개수의 비율을 의미할 수 있고, P_{ν_1}은 N에 대한 제2-1광자의 개수의 비율을 의미할 수 있고, P_{ν_2}는 N에 대한 제2-2광자의 개수의 비율을 의미할 수 있고, P_{ν_3}는 N에 대한 제2-3광자의 개수의 비율을 의미할 수 있고, P_{ν_4}는 N에 대한 제2-4광자의 개수의 비율을 의미할 수 있다. 제1값(μ), 제2-1값(ν_1), 제2-2값(ν_2), 제2-3값(ν_3), 및 제2-4값(ν_4)은 각각 신호 상태의 평균광자수, 제1미끼 상태의 평균광자수, 제2미끼 상태의 평균광자수, 제3미끼 상태의 평균광자수, 및 제4미끼 상태의 평균광자수를 의미할 수 있다. 일 실시예에 따라, 프로세서(120)는 MATLAB의 기 설정된 함수를 이용하여 보안 용량이 최대가 되도록 하는 복수의 파라미터들을 확인할 수 있다. 예를 들어, 기 설정된 함수는 fmicon 함수를 포함할 수 있다. 일 실시예에 따라 확인된 복수의 파라미터들은 아래 표 1 및 표 2로 나타낼 수 있다.

[0081] [표 1]

N	10^{12}	10^{14}	10^{16}
μ	0.20502	0.212247	0.214422
ν_1	0.153765	0.159185	0.160816
ν_2	0.079003	0.081788	0.082626
ν_3	0.007868	0.003273	0.001182
P_μ	0.928245	0.982816	0.995502
P_{ν_1}	0.019654	0.004129	0.000883
P_{ν_2}	0.023117	0.004761	0.001009
P_{ν_3}	0.026234	0.007231	0.002154
P_{vac}	0.00275	0.001063	0.000451
C_s	0.002121	0.002556	0.002672

[0082]

[0083] [표 2]

N	10^{12}	10^{14}	10^{16}
μ	0.120382	0.128326	0.130623
ν_1	0.090286	0.096245	0.097967
ν_2	0.046388	0.04945	0.050335
ν_3	0.006735	0.003385	0.001288
P_μ	0.866041	0.969617	0.992299
P_{ν_1}	0.036942	0.007619	0.001623
P_{ν_2}	0.045093	0.009065	0.0019
P_{ν_3}	0.046571	0.011874	0.00343
P_{vac}	0.005353	0.001824	0.000747
C_s	0.000491	0.000703	0.00076

[0084]

[0085] 표 1 및 표 2를 참조하면, 기 설정된 개수의 광자(N)에 대해 보안 용량(C_s)을 최대화하는 복수의 파라미터 값을

확인할 수 있다. 표 1 및 표 2의 P_{vac}는 N에 대한 제2-4광자의 개수의 비율(P_{v_4})을 의미할 수 있다. 표 1은 양자 채널의 손실이 1dB인 경우의 복수의 파라미터의 값들을 나타내고, 표 2는 양자 채널의 손실이 3dB인 경우의 복수의 파라미터 값들을 나타낸다. 예를 들어, 표 1에서 N이 10^{12} 인 경우, 최대가 되는 보안 용량(C_s)은 0.002121임을 확인할 수 있고, 제1값(μ), 제2-1값(ν_1), 제2-2값(ν_2), 제2-3값(ν_3)이 각각 0.153765, 0.079003, 0.007868 일 때 보안 용량(C_s)이 최대가 된다는 것을 확인할 수 있다.

[0087] 도 3은 일 실시예에 따라 계산된 보안 용량의 그래프를 나타낸다.

[0088] 도 3을 참조하면, x축은 양자 채널의 손실을 나타내고 y축은 펄스 당 계산된 보안 용량을 나타낸다. 파선으로 이루어진 곡선은 데이터 사이즈를 무한으로 가정했을 때 계산된 보안 용량 곡선을 나타낼 수 있다. 실선으로 이루어진 곡선들은 데이터 사이즈를 유한(예를 들어, $10^{16}, 10^{14}, 10^{12}, 10^{11}$)으로 가정했을 때 계산된 보안 용량 곡선을 나타낼 수 있다. 본 개시는 유한한 데이터 사이즈를 사용할 때 발생하는 통계적 변동을 고려하여 실선으로 이루어진 보안 용량 곡선들을 확인함으로써 보다 실용적인 양자직접통신을 구현할 수 있다.

[0090] 도 4는 일 실시예에 따른 전자 장치의 동작 방법을 나타낸다.

[0091] 단계 S410에서, 전자 장치는 양자직접통신을 위한 프로토콜에 따른 도청에 의해 간섭 받는 양자직접통신에 관한 시뮬레이션을 수행할 수 있다.

[0092] 단계 S420에서, 전자 장치는 시뮬레이션 결과를 기초로, 평균광자수(Mean Photon Number)가 제1값인 신호 상태(signal state)일 때 시뮬레이션에서의 수신 장치가 생성한 레이저 펄스에 포함되는 제1광자가 제1경로를 통해 수신 장치에서 검출되는 확률에 관한 제1정보, 제1광자가 제2경로를 통해 도청을 수행하는 도청 장치에서 검출되는 확률에 관한 제2정보, 및 에러율에 관한 정보를 확인할 수 있다.

[0093] 단계 S430에서, 전자 장치는 가우시안 근사(Gaussian Approximation)를 이용하여 제1정보, 제2정보, 및 에러율에 관한 정보의 상한 및 하한 중 적어도 하나를 계산하고, 제1정보, 제2정보, 및 에러율에 관한 정보의 상한 및 하한 중 적어도 하나에 기초하여 프로토콜의 보안 용량(Secrecy Capacity)을 계산할 수 있다.

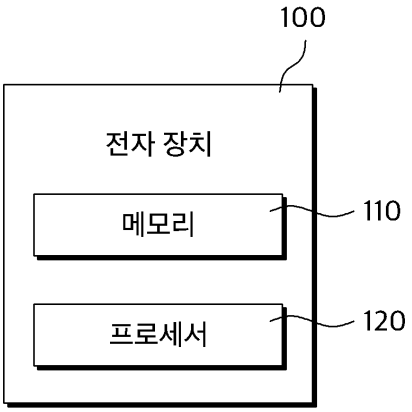
[0094] 전술한 실시예들에 따른 전자 장치는, 프로세서, 프로그램 데이터를 저장하고 실행하는 메모리, 디스크 드라이브와 같은 영구 저장부(permanent storage), 외부 장치와 통신하는 통신 포트, 터치 패널, 키(key), 버튼 등과 같은 사용자 인터페이스 장치 등을 포함할 수 있다. 소프트웨어 모듈 또는 알고리즘으로 구현되는 방법들은 상기 프로세서상에서 실행 가능한 컴퓨터가 읽을 수 있는 코드들 또는 프로그램 명령들로서 컴퓨터가 읽을 수 있는 기록 매체 상에 저장될 수 있다. 여기서 컴퓨터가 읽을 수 있는 기록 매체로 마그네틱 저장 매체(예컨대, ROM(read-only memory), RAM(random-Access memory), 플로피 디스크, 하드 디스크 등) 및 광학적 판독 매체(예컨대, 시디롬(CD-ROM), 디브이디(DVD: Digital Versatile Disc)) 등이 있다. 컴퓨터가 읽을 수 있는 기록 매체는 네트워크로 연결된 컴퓨터 시스템들에 분산되어, 분산 방식으로 컴퓨터가 판독 가능한 코드가 저장되고 실행될 수 있다. 매체는 컴퓨터에 의해 판독가능하며, 메모리에 저장되고, 프로세서에서 실행될 수 있다.

[0095] 본 실시예는 기능적인 블록 구성들 및 다양한 처리 단계들로 나타내어질 수 있다. 이러한 기능 블록들은 특정 기능들을 실행하는 다양한 개수의 하드웨어 또는/및 소프트웨어 구성들로 구현될 수 있다. 예를 들어, 실시예는 하나 이상의 마이크로프로세서들의 제어 또는 다른 제어 장치들에 의해서 다양한 기능들을 실행할 수 있는, 메모리, 프로세싱, 로직(logic), 룩 업 테이블(look-up table) 등과 같은 직접 회로 구성들을 채용할 수 있다. 구성 요소들이 소프트웨어 프로그래밍 또는 소프트웨어 요소들로 실행될 수 있는 것과 유사하게, 본 실시 예는 데이터 구조, 프로세스들, 루틴들 또는 다른 프로그래밍 구성들의 조합으로 구현되는 다양한 알고리즘을 포함하여, C, C++, 자바(Java), 어셈블러(assembler) 등과 같은 프로그래밍 또는 스크립팅 언어로 구현될 수 있다. 기능적인 측면들은 하나 이상의 프로세서들에서 실행되는 알고리즘으로 구현될 수 있다. 또한, 본 실시 예는 전자적인 환경 설정, 신호 처리, 및/또는 데이터 처리 등을 위하여 종래 기술을 채용할 수 있다. “매커니즘”, “요소”, “수단”, “구성”과 같은 용어는 넓게 사용될 수 있으며, 기계적이고 물리적인 구성들로서 한정되는 것은 아니다. 상기 용어는 프로세서 등과 연계하여 소프트웨어의 일련의 처리들(routines)의 의미를 포함할 수 있다.

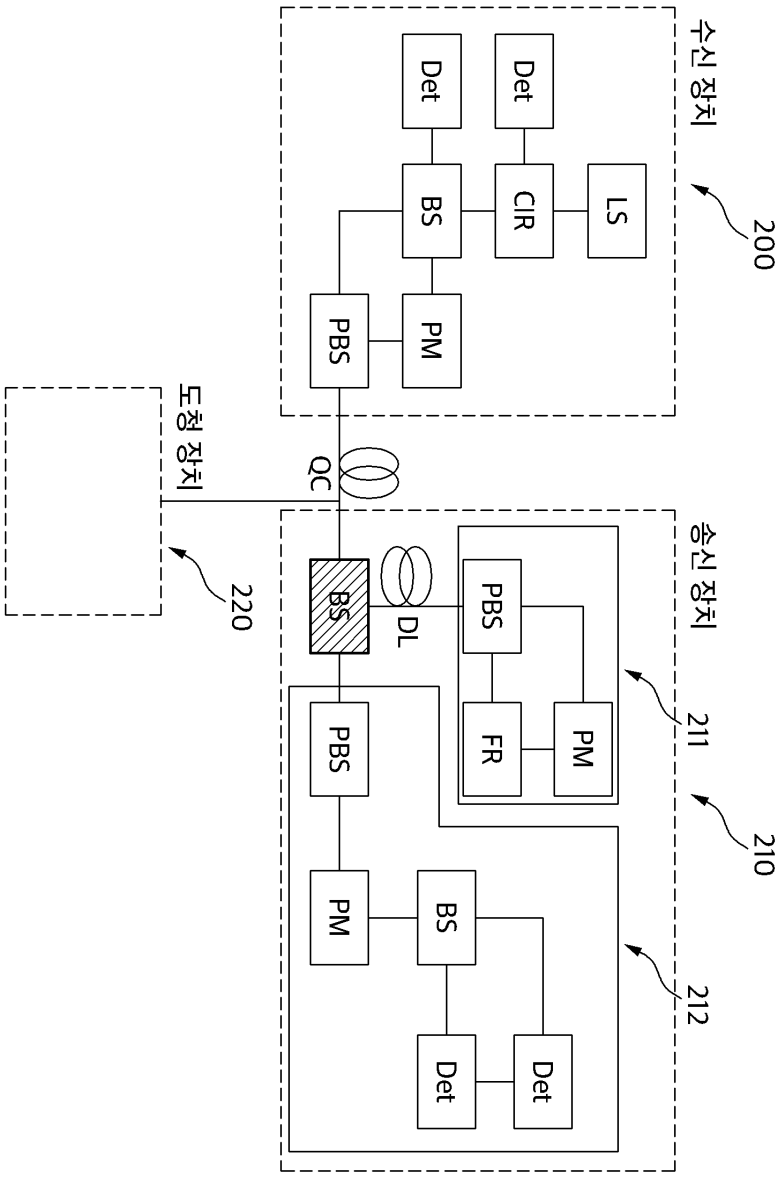
[0096] 전술한 실시예들은 일 예시일 뿐 후술하는 청구항들의 범위 내에서 다른 실시예들이 구현될 수 있다.

도면

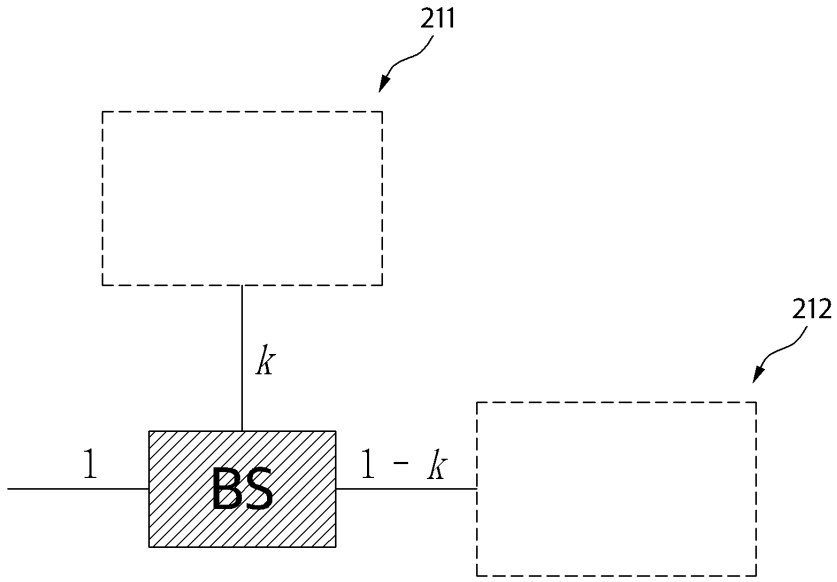
도면1



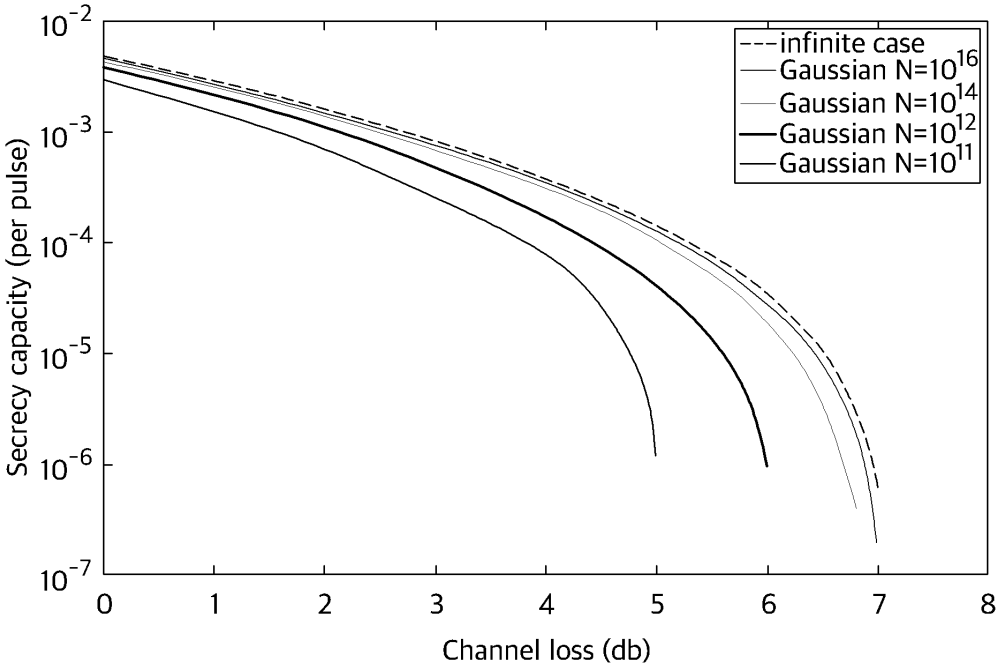
도면2a


수신 장치
200
Det
Det
BS
CIR
LS
PBS
PM
도청 장치
220
QC
송신 장치
210
211
212
BS
DL
PBS
FR
PM
PBS
PM
BS
Det
Det

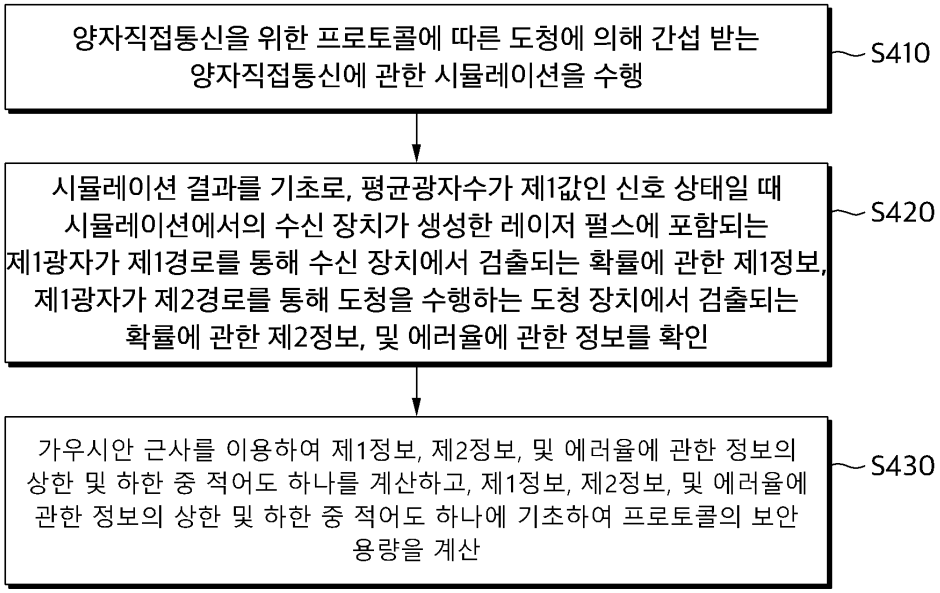
도면2b


211
212
k
1
BS
1 - k

도면3


infinite case
Gaussian N=10^16
Gaussian N=10^14
Gaussian N=10^12
Gaussian N=10^11
Secrecy capacity (per pulse)
Channel loss (db)
10^-2
10^-3
10^-4
10^-5
10^-6
10^-7
0
1
2
3
4
5
6
7
8

도면4


양자직접통신을 위한 프로토콜에 따른 도청에 의해 간섭 받는 양자직접통신에 관한 시뮬레이션을 수행
S410
시뮬레이션 결과를 기초로, 평균광자수가 제1값인 신호 상태일 때 시뮬레이션에서의 수신 장치가 생성한 레이저 펄스에 포함되는 제1광자가 제1경로를 통해 수신 장치에서 검출되는 확률에 관한 제1정보, 제1광자가 제2경로를 통해 도청을 수행하는 도청 장치에서 검출되는 확률에 관한 제2정보, 및 에러율에 관한 정보를 확인
S420
가우시안 근사를 이용하여 제1정보, 제2정보, 및 에러율에 관한 정보의 상한 및 하한 중 적어도 하나를 계산하고, 제1정보, 제2정보, 및 에러율에 관한 정보의 상한 및 하한 중 적어도 하나에 기초하여 프로토콜의 보안 용량을 계산
S430