

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)(11) 공개번호 10-2023-0149628
(43) 공개일자 2023년10월27일

(51) 국제특허분류(Int. Cl.)
H04B 10/70 (2013.01) H04B 10/079 (2013.01)
H04B 10/85 (2013.01) H04L 9/08 (2006.01)
(52) CPC특허분류
H04B 10/70 (2013.01)
H04B 10/0795 (2013.01)
(21) 출원번호 10-2022-0049079
(22) 출원일자 2022년04월20일
심사청구일자 2022년04월20일

(71) 출원인
경희대학교 산학협력단
경기도 용인시 기흥구 덕영대로 1732 (서천동, 경희대학교 국제캠퍼스내)
(72) 발명자
신현동
경기도 수원시 영통구 청명로 132, 323동 501호(영통동, 벽산삼익아파트)
자만 파카
경기도 용인시 기흥구 덕영대로 1732, 전자정보관 559호
서 낭 파잉
경기도 수원시 영통구 청명남로50번길 13-12, 101호
(74) 대리인
김연권

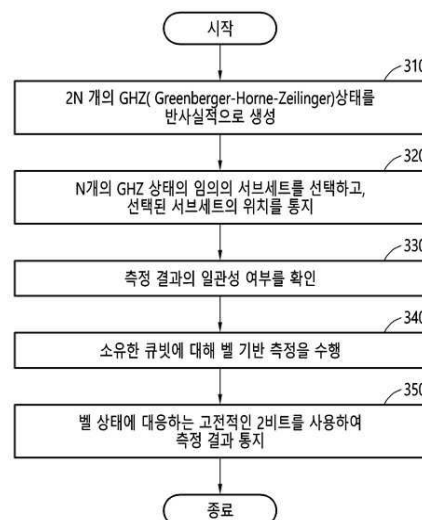
전체 청구항 수 : 총 6 항

(54) 발명의 명칭 양자 정보 처리 통합 시스템에서 제어된 반사실적 양자 순간이동 지원 장치 및 방법

(57) 요약

양자 정보 처리 통합 시스템에서 제어된 반사실적 양자 순간이동 지원 장치 및 방법을 개시한다. 송신 단말에서 수행되는 제어된 반사실적 양자 순간이동 지원 방법은 2N 개의 GHZ(Greenberger-Horne-Zeilinger)상태를 반사실적으로 생성하는 단계와, N개의 GHZ 상태의 임의의 서브세트를 선택하고, 선택된 서브세트의 위치를 수신 단말 및 제어 단말로 통지하는 단계와, 상기 수신 단말 및 제어 단말의 큐빗 측정 결과를 수신하고 측정 결과의 일관성을 확인하는 단계 및 상기 측정 결과의 일관성이 기 설정된 임계 값까지 신뢰 가능한 경우 자신이 소유한 큐빗에 대해 벨 기반 측정을 수행함으로써, 미지의 양자상태를 순간이동 시키는 단계를 포함한다.

대표도 - 도3



(52) CPC특허분류

H04B 10/85 (2013.01)

H04L 9/0852 (2023.08)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711155671
과제번호	2019R1A2C2007037
부처명	과학기술정보통신부
과제관리(전문)기관명	한국연구재단
연구사업명	(유형1-2)중견연구
연구과제명	양자네트워킹 핵심기술 연구
기 여 율	70/100
과제수행기관명	경희대학교 산학협력단
연구기간	2019.03.01 ~ 2024.02.29

이 발명을 지원한 국가연구개발사업

과제고유번호	1711152558
과제번호	2021-0-02046-002
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	정보통신기술인력양성/대학ICT연구센터육성지원
연구과제명	6H 차세대 이동통신 기술 개발
기 여 율	30/100
과제수행기관명	경희대학교 산학협력단
연구기간	2021.07.01 ~ 2028.12.31

명세서

청구범위

청구항 1

2N 개의 GHZ(Greenberger-Horne-Zeilinger)상태를 반사실적으로 생성하는 단계;

N개의 GHZ 상태의 임의의 서브세트를 선택하고, 선택된 서브세트의 위치를 수신 단말 및 제어 단말로 통지하는 단계;

상기 수신 단말 및 제어 단말의 큐빗 측정 결과를 수신하고 측정 결과의 일관성을 확인하는 단계; 및

상기 측정 결과의 일관성이 기 설정된 임계 값까지 신뢰 가능한 경우 자신이 소유한 큐빗에 대해 벨 기반 측정을 수행함으로써, 미지의 양자상태를 순간이동 시키는 단계를 포함하는

양자 정보 처리 통합 시스템에서 송신 단말에서 수행되는 제어된 반사실적 양자 순간이동 지원 방법.

청구항 2

제1항에 있어서,

상기 제어 단말은 Hadamard 기저로 큐빗을 측정하고 미지의 양자 상태를 재구성하도록 수신 단말에게 측정 결과를 통지하는 것을 특징으로 하는

양자 정보 처리 통합 시스템에서 송신 단말에서 수행되는 제어된 반사실적 양자 순간이동 지원 방법.

청구항 3

제2항에 있어서,

상기 제어 단말은 제어된 반사실적 양자 순간이동을 승인하기 위해 고전적 정보인 m의 1비트를 통해 상기 측정 결과를 통지하는

양자 정보 처리 통합 시스템에서 송신 단말에서 수행되는 제어된 반사실적 양자 순간이동 지원 방법.

청구항 4

제3항에 있어서,

상기 제어 단말에 의해 통신이 승인되면, 벨 상태 $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$ 에 대응하는 $\{00, 01, 10, 11\}$ 세트로부터 고전적 정보인 m1m2 2비트를 통해 측정 결과를 상기 수신 단말에게 통지하는

양자 정보 처리 통합 시스템에서 송신 단말에서 수행되는 제어된 반사실적 양자 순간이동 지원 방법.

청구항 5

제4항에 있어서,

상기 수신 단말은 양자 상태를 재구성하기 위해 상기 송신 단말 및 제어 단말의 측정 결과에 기초하여 큐빗 r_j 에서 수학적 식 4와 같이 정의되는 유니터리 오퍼레이션(unitary operation)을 수행하는,

[수학적 식 4]

$$U = X^{m_1} Z^{m_2+m}$$

여기서, X 및 Z는 각각 Pauli x 및 z 연산자를 의미하는

양자 정보 처리 통합 시스템에서 송신 단말에서 수행되는 제어된 반사실적 양자 순간이동 지원 방법.

청구항 6

2N 개의 GHZ(Greenberger-Horne-Zeilinger)상태를 반사실적으로 생성하고, N개의 GHZ 상태의 임의의 서브세트를 선택하고, 선택된 서브세트의 위치를 수신 단말 및 제어 단말로 통지하고, 상기 수신 단말 및 제어 단말의 큐비트 측정 결과를 수신하고 측정 결과의 일관성이 기 설정된 임계 값까지 신뢰 가능한 경우 자신이 소유한 큐비트에 대해 벨 기반 측정을 수행함으로써, 미지의 양자상태를 순간이동 시키는 반사실 양자 통신 처리부를 포함하는 양자 통신 플랫폼 및

추정될 양자 상태를 양자 스위치로 전송하고, 상기 양자 스위치에서 출력되는 상태에서 양자 상태 단층 촬영을 수행하고, 상기 양자 상태 단층 촬영의 출력 및 대수학에 기반하여 초기 상태를 추정하는 양자 상태 단층 촬영 처리부를 포함하는 양자 관측 및 분석 플랫폼을 포함하는

양자 정보 처리 통합 시스템.

발명의 설명

기술 분야

[0001] 기술 분야는 제어된 반사실적 양자 순간이동 지원 장치 및 방법에 관한 것이다. 제어된 반사실적 양자 순간이동 지원 장치 및 방법은 양자정보기술 통합 시스템에서 양자통신 플랫폼의 반사실 양자통신 처리부에 적용될 수 있다.

배경 기술

[0002] 양자 순간이동(quantum teleportation)은 광자의 양자 얽힘을 이용해 양자정보를 한 곳에서 사라지게 하고 다른 곳에서 나타나게 하는 전송 방법으로 양자컴퓨터와 양자 통신 등에 응용될 수 있는 기술이다.

[0003] 양자 순간이동은 다양한 양자 정보 처리 기술에 필수적인 자원이라 할 수 있다. 양자 순간이동을 이용하여 네트워크 참가자는 서로 다른 노드 사이에서 미지의 양자 상태를 전송할 수 있다.

[0004] 1993년 Bennett et al.은 공유 EPR(Einstein-Pidolsky-Rosen) 쌍과 2비트의 고전적 정보 전송을 사용하여 한 장소에서 원격 장소로 미지의 양자 상태를 전송하는 최초의 프로토콜을 제시한 바 있다. 이후, 공유 EPR 쌍 대신 공유 GHZ(Greenberger-Horne-Zeilinger) 상태를 사용하는 제어 방식 등 지금까지 제어된 양자 상태 전달에 대한 다양한 연구가 진행되었다.

[0005] 종래기술에 따른 양자 순간이동은 미지의 양자상태의 순간 이동을 가능하게 하기 위해 채널을 통해 물리적 입자를 보내어 얽힘을 공유하는 공통점을 갖고 있다. 종래기술과 달리 GHZ 상태가 송수신 단말 및 관리자 단말 간에 비지역적으로 공유될 수 있는 반사실적 양자 순간이동을 구현할 필요가 있다.

[0006] 또한, 제어된 반사실적 양자 순간이동 뿐만 아니라 관련된 기술의 구현 및 연구를 지원하기 위한 다양한 양자 정보 처리를 지원할 수 있는 양자 정보 통합 시스템이 필요하다.

선행기술문헌

특허문헌

[0007] (특허문헌 0001) 한국 등록특허 제10-2017839호(2019년 08월 28일, 반사실적 양자 벨 분석 방법, 장치 및 시스템)

(특허문헌 0002) 미국 등록특허 제8,891,767호(Nov. 18, 2014, METHOD AND APPARATUS FOR DIRECT COUNTERFACTUAL QUANTUM COMMUNICATION)

발명의 내용

해결하려는 과제

[0008] 본 발명은 반사실적으로 즉, 채널을 통해 물리적 입자를 전송하지 않고 당사자들 사이에서 얽힘을 공유할 수 있는 제어된 반사실적 양자 순간이동 지원 장치 및 방법을 제공하는 것을 목적으로 한다.

[0009] 또한, 본 발명은 제어된 반사실적 양자 순간이동 뿐만 아니라 관련된 기술의 구현 및 연구를 지원하기 위한 다

양한 양자 정보 처리를 지원할 수 있는 양자 정보 통합 시스템을 제공하는 것을 목적으로 한다.

과제의 해결 수단

- [0010] 일 실시예에 따른 송신 단말에서 수행되는 제어된 반사실적 양자 순간이동 지원 방법은 $2N$ 개의 GHZ(Greenberger-Horne-Zeilinger)상태를 반사실적으로 생성하는 단계와, N 개의 GHZ 상태의 임의의 서브세트를 선택하고, 선택된 서브세트의 위치를 수신 단말 및 제어 단말로 통지하는 단계와, 상기 수신 단말 및 제어 단말의 큐비트 측정 결과를 수신하고 측정 결과의 일관성을 확인하는 단계 및 상기 측정 결과의 일관성이 기 설정된 임계값까지 신뢰 가능한 경우 자신이 소유한 큐비트에 대해 벨 기반 측정을 수행함으로써, 미지의 양자상태를 순간이동 시키는 단계를 포함한다.
- [0011] 상기 제어 단말은 Hadamard 기저로 큐비트를 측정하고 미지의 양자 상태를 재구성하도록 수신 단말에게 측정 결과를 통지할 수 있다.
- [0012] 상기 제어 단말은 제어된 반사실적 양자 순간이동을 승인하기 위해 고전적 정보인 m 의 1비트를 통해 상기 측정 결과를 통지할 수 있다.
- [0013] 상기 제어 단말에 의해 통신이 승인되면, 벨 상태 $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$ 에 대응하는 $\{00, 01, 10, 11\}$ 세트로부터 고전적 정보인 $m1m2$ 2비트를 통해 측정 결과를 상기 수신 단말에게 통지할 수 있다.
- [0014] 상기 수신 단말은 양자 상태를 재구성하기 위해 상기 송신 단말 및 제어 단말의 측정 결과에 기초하여 큐비트 r_j 에 서 수학적 4와 같이 정의되는 유니터리 오퍼레이션(unitary operation)을 수행할 수 있다.

발명의 효과

- [0015] 본 발명의 실시예에 따르면, 채널을 통해 물리적 입자를 전송하지 않고 당사자들 사이에서 얽힘을 공유할 수 있다.
- [0016] 본 발명의 실시예에 따르면, 반사실적 속성과 측정의 일관성 검사로 인해 다양한 도청 전략에 대한 저항력이 개선되는 효과를 갖는다.
- [0017] 본 발명의 실시예에 따르면, 제어된 반사실적 양자 순간이동 뿐만 아니라 관련된 기술의 구현 및 연구를 지원하기 위한 다양한 양자 정보 처리를 지원할 수 있다.

도면의 간단한 설명

- [0018] 도 1은 본 발명의 실시예에 따른 반사실적 얽힘 분배(Counterfactual Entanglement Distribution) 모델을 설명하기 위한 도면이다.
- 도 2는 본 발명의 실시예에 따른 제어된 양자 순간이동의 개념을 나타내는 도면이다.
- 도 3은 본 발명의 실시예에 따른 제어된 반사실적 양자 순간이동 지원 장치의 동작을 나타내는 흐름도이다.
- 도 4는 큐비트 전송에서 QST를 수행하기 위한 메커니즘을 설명하는 도면이다.
- 도 5는 순수 상태들 (a)과 혼합 상태들 (b)에 대한 재구성 상태와 실제 상태 의 Log 부정확도(infidelity)를 나타낸다.
- 도 6은 본 발명의 일실시예에 따른 단층 촬영 장치의 블록도이다.
- 도 7은 본 발명의 실시예에 따른 양자정보기술 통합 시스템을 나타내는 도면이다.

발명을 실시하기 위한 구체적인 내용

- [0019] 이하 첨부 도면들 및 첨부 도면들에 기재된 내용들을 참조하여 본 발명의 실시예를 상세하게 설명하지만, 본 발명이 실시예에 의해 제한되거나 한정되는 것은 아니다.
- [0020] 본 명세서에서 사용된 용어는 실시예들을 설명하기 위한 것이며 본 발명을 제한하고자 하는 것은 아니다. 본 명세서에서, 단수형은 문구에서 특별히 언급하지 않는 한 복수형도 포함한다. 명세서에서 사용되는 "포함한다(comprises)" 및/또는 "포함하는(comprising)"은 언급된 구성요소, 단계, 동작 및/또는 소자는 하나 이상의 다른 구성요소, 단계, 동작 및/또는 소자의 존재 또는 추가를 배제하지 않는다.

- [0021] 본 명세서에서 사용되는 “실시예”, “예”, “측면”, “예시” 등은 기술된 임의의 양상(Aspect) 또는 설계가 다른 양상 또는 설계들보다 양호하다거나, 이점이 있는 것으로 해석되어야 하는 것은 아니다.
- [0022] 또한, '또는' 이라는 용어는 배타적 논리합 'exclusive or' 이기보다는 포함적인 논리합 'inclusive or' 를 의미한다. 즉, 달리 언급되지 않는 한 또는 문맥으로부터 명확하지 않는 한, 'x가 a 또는 b를 이용한다' 라는 표현은 포함적인 자연 순열들(natural inclusive permutations) 중 어느 하나를 의미한다.
- [0023] 또한, 본 명세서 및 청구항들에서 사용되는 단수 표현("a" 또는 "an")은, 달리 언급하지 않는 한 또는 단수 형태에 관한 것이라고 문맥으로부터 명확하지 않는 한, 일반적으로 "하나 이상"을 의미하는 것으로 해석되어야 한다.
- [0024] 또한, 본 명세서 및 청구항들에서 사용되는 제1, 제2 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다.
- [0025] 다른 정의가 없다면, 본 명세서에서 사용되는 모든 용어(기술 및 과학적 용어를 포함)는 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에게 공통적으로 이해될 수 있는 의미로 사용될 수 있을 것이다. 또 일반적으로 사용되는 사전에 정의되어 있는 용어들은 명백하게 특별히 정의되어 있지 않는 한 이상적으로 또는 과도하게 해석되지 않는다.
- [0026] 한편, 본 발명을 설명함에 있어서, 관련된 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는, 그 상세한 설명을 생략할 것이다. 그리고, 본 명세서에서 사용되는 용어(terminology)들은 본 발명의 실시예를 적절히 표현하기 위해 사용된 용어들로서, 이는 사용자, 운용자의 의도 또는 본 발명이 속하는 분야의 관례 등에 따라 달라질 수 있다. 따라서, 본 용어들에 대한 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.
- [0028] 도 1은 본 발명의 실시예에 따른 반사실적 얽힘 분배(Counterfactual Entanglement Distribution) 모델을 설명하기 위한 도면이다.
- [0029] 도 1을 참조하면, 제1 단말(Alice)(110), 제2 단말(Bob)(120) 및 제3 단말(Charlie)(130) 각각은 모두 송신 단말, 수신 단말 및 제어 단말로 동작할 수 있다. 예를 들어, Alice(110)가 Bob(120)에게 양자 정보를 보내는 경우 Charlie(130)는 제어 단말의 역할을 수행하고, 반대로 Bob(120)이 Alice(130)에게 양자 정보를 보내는 경우도 가능하다. 이와 같이, 본 발명의 실시예에 따른 제어된 양자 순간 이동 프로토콜은 3자 양자네트워크를 구성한다.
- [0030] 한편, 도 1에서 참조부호 140 'SW'는 전환 가능 미러(Switchable Mirror)의 및 전환 가능 회전자 등을 포함하는 양자 채널을 의미하고, QA0는 quantum absorptive object의 약칭이고, V-CQZ는 수직(Vertical) CQZ 게이트를 포함함을 나타내고, H-CQZ는 수평(Horizontal) CQZ 게이트를 포함하고 있음을 나타낸다.
- [0032] **[제1 단계]**
- [0033] 제1 단계에서 각 단말은 2N 개의 GHZ 상태를 반사실적으로 생성한다.
- [0034] 제어된 반사실적 양자 순간이동을 안전하게 수행하기 위하여, Alice, Bob 및 Charlie는 CQZ (Counterfactual quantum Zeno) gate를 사용하여 2N GHZ 상태를 반사실적으로 생성한다. 여기서, N은 자연수를 나타내고, 각 단말은 2N GHZ 상태의 큐비트를 하나씩 갖는 2N 삼각(tripartite) GHZ 상태를 생성한다.
- [0035] 송신 단말로 가정된 Alice는 얽힘을 반사실적으로 분배하기 위하여, GHZ 상태 생성의 각 라운드에서 자신의 큐비트가 양자 흡수 객체(quantum absorptive object, QA0)로 동작하는 $|\psi\rangle_A = (|0\rangle_A + |1\rangle_A) / 2$ 상태에서 큐비트를 준비한다. 이때, Bob과 Charlie는 각각 $|0\rangle_B$ 및 $|1\rangle_C$ 인 상태에서 큐비트를 준비한다.
- [0036] Bob과 Charlie는 도 1에 도시된 바와 같이, GHZ 상태 생성의 각 라운드에서 CQZ 게이트를 사용하여 양자 채널을 통해 Alice와 교대로 연결한다.

[0037] 각 라운드가 종료되는 시점에 Alice, Bob 및 Charlie의 초기 상태는 수학적 식 1과 같이 변환된다.

[0038] [수학적 식 1]

$$|\theta\rangle_{A_i B_i C_i} = \frac{1}{\sqrt{2}} (|000\rangle_{A_i B_i C_i} + |111\rangle_{A_i B_i C_i})$$

$$i \in \{1, 2, \dots, 2N\}$$

[0041] 여기서, A, B, C는 각각 Alice, Bob 및 Charlie를 나타내는 인덱스이고, i는 GHZ 상태 생성의 i번째 라운드를 나타내는 인덱스를 의미한다.

[제2 단계]

[0044] 제2 단계에서 Alice, Bob 및 Charlie는 큐비트 측정 및 결과발표를 수행한다.

[0045] 먼저, Alice는 보안 검사를 위하여, 2N개의 GHZ 상태들 중 N개의 GHZ 상태의 임의의 서브세트를 선택하고, 선택된 서브세트의 위치를 통지(announce) 한다.

[0046] Bob 및 Charlie는 {x, y} 세트로부터 측정 기저(basis)을 랜덤하게 선택하여 각 큐비트에서 측정을 수행하고 측정 결과와 선택한 기저(basis) 세트를 통지한다.

[0047] Alice는 [표 1]과 같은 Bob 및 Charlie의 측정 후 측정 결과 테이블을 참조하여 Bob 및 Charlie의 측정 결과를 비교하거나 매칭한다. 이를 통해 측정 결과의 일관성 여부를 확인할 수 있다.

표 1

		Bob			
		+x	-x	+y	-y
Charlie	+x	$ 0\rangle + 1\rangle$	$ 0\rangle - 1\rangle$	$ 0\rangle - i 1\rangle$	$ 0\rangle + i 1\rangle$
	-x	$ 0\rangle - 1\rangle$	$ 0\rangle + 1\rangle$	$ 0\rangle + i 1\rangle$	$ 0\rangle - i 1\rangle$
	+y	$ 0\rangle - i 1\rangle$	$ 0\rangle + i 1\rangle$	$ 0\rangle - 1\rangle$	$ 0\rangle + 1\rangle$
	-y	$ 0\rangle + i 1\rangle$	$ 0\rangle - i 1\rangle$	$ 0\rangle + 1\rangle$	$ 0\rangle - 1\rangle$

Alice's measurement result

[0048]

[0049] 측정 결과의 일관성이 기 설정된 허용 가능한 임계 값까지 신뢰 가능한 경우, Alice, Bob 및 Charlie는 다음 단계를 수행할 수 있다. 즉, Alice, Bob 및 Charlie는 다음 단계에서 선택된 서브 세트 이외의 N개의 GHZ 상태를 사용하여 임의의 알려지지 않은 큐비트를 삼각 양자 네트워크(tripartite quantum network)에서 전송할 수 있다.

[0050] 한편, 각 당사자는 송신 단말, 수신 단말 및 제어 단말로 동작할 수 있음을 고려하여, 이후의 명세서 상의 기재에서 GHZ 상태의 첨자는 s, r, c로 표현하기로 한다. 여기서, s, r, c는 각각 송신 단말, 수신 단말 및 제어 단말에 구비된(혹은 해당 단말이 소유한) 큐비트를 나타낸다.

[제3 단계]

[0053] 제3 단계에서 송신 단말은 자신이 소유한 큐비트에 대해 벨 기반 측정을 수행함으로써, 미지의 양자상태를 순간이동 시킨다. 보다 구체적으로, 수학적 식 2와 같이 정의되는 미지의 양자 상태 $|\phi\rangle_q$ 를 송신 단말이 전송하는 경우를 가정한다.

[0054] [수학적 식 2]

$$|\phi\rangle_q = \alpha |0\rangle_q + \beta |1\rangle_q,$$

$$|\alpha|^2 + |\beta|^2 = 1.$$

[0056]

[0057] 미지의 양자 상태 및 GHZ 상태의 조합 상태는 수학적식 3과 같이 표현될 수 있다.

[0058] [수학적식 3]

$$\begin{aligned} |\eta_j\rangle &= |\phi\rangle_q \otimes |\theta\rangle_{s_j r_j c_j} \\ &= \frac{1}{2} \left[|\Phi^+\rangle_{qs_j} \otimes (\alpha |00\rangle_{r_j c_j} + \beta |11\rangle_{r_j c_j}) \right. \\ &\quad + |\Phi^-\rangle_{qs_j} \otimes (\alpha |00\rangle_{r_j c_j} - \beta |11\rangle_{r_j c_j}) \\ &\quad + |\Psi^+\rangle_{qs_j} \otimes (\alpha |11\rangle_{r_j c_j} + \beta |00\rangle_{r_j c_j}) \\ &\quad \left. + |\Psi^-\rangle_{qs_j} \otimes (\alpha |11\rangle_{r_j c_j} - \beta |00\rangle_{r_j c_j}) \right], \end{aligned}$$

$$j \in \{1, 2, \dots, N\}.$$

[0061] 여기서, $|\Phi^\pm\rangle$ 및 $|\Psi^\pm\rangle$ 는 벨 상태를 나타내고, j는 제어된 양자 순간 이동의 j번째 라운드를 나타낸다.

[0062] 제3 단계에서 송신 단말은 큐비트 q 및 s_j 에 대한 벨 기저 측정을 수행하고, 측정 결과를 기록 및 유지한다.

[제4 단계]

[0065] 제4 단계에서 제어 단말은 Hadamard 기저로 큐비트를 측정하고 미지의 양자 상태를 재구성하도록 수신단말에게 측정 결과를 통지한다.

[0066] 보다 구체적으로, 제어 단말은 큐비트 c_j 에서 Hadamard gate H를 수행하고 계산 기저로 큐비트를 측정한다. 제어 단말은 제어된 반사실적 양자 순간이동을 승인하기 위해 고전적 정보인 m의 1비트를 통해 측정 결과를 통지한다.

[0067] 제어 단말이 송신 단말과 수신 단말 간의 통신을 승인하면, 송신 단말은 벨 상태 $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$ 에 대응하는 $\{00, 01, 10, 11\}$ 세트로부터 고전적 정보인 $m_1 m_2$ 2비트를 통해 측정 결과를 제어 단말 및 수신 단말에게 통지한다.

[0068] 도 2는 본 발명의 실시예에 따른 제어된 양자 순간이동의 개념을 나타내는 도면이다.

[0069] 도 2를 참조하면, 제어 단말의 승인하에 송신 단말은 벨 측정 결과를 통지함으로써, 제어된 양자 순간이동을 수행함을 알 수 있다.

[제5 단계]

[0072] 제5 단계에서 수신 단말은 양자 상태를 재구성한다.

[0073] 보다 구체적으로, 수신 단말은 양자 상태를 재구성하기 위해 송신 단말 및 제어 단말의 측정 결과에 기초하여 큐비트 r_j 에서 수학적식 4와 같이 정의되는 유니터리 오퍼레이션(unitary operation)을 수행한다.

[0074] [수학적식 4]

$$U = X^{m_1} Z^{m_2+m}$$

[0076] 여기서, X 및 Z는 각각 Pauli x 및 z 연산자를 의미한다.

[0077] 제1 단계 내지 제5단계를 통해 설명된 방법은 제어를 수행하는 제어 단말의 승인하에 미지의 양자 상태 시퀀스를 재구성할 수 있다. 따라서, 다양한 공격 전략에 대해 보다 안전하고 다자간 통신 시스템에 활용이 가능하다.

[0078] 만일, 도청을 시도하는 단말이 얽힘 분배 과정에 참여하려고 시도하는 경우, 얽힘 관계에 있을 수 있지만 제2

단계의 보안 검사 과정에서 도청을 시도하는 단말이 탐지될 수 있다.

- [0079] 또한, 도청을 시도하는 단말이 Alice의 미지 양자 상태를 훔치기 위해 보이지 않는 광자를 추가하는 경우, 보이지 않는 광자로 인해 보안 검사 단계에서 더 많은 오류가 발생할 수 있다.
- [0081] 도 3은 본 발명의 실시예에 따른 제어된 반사실적 양자 순간이동 지원 장치의 동작을 나타내는 흐름도이다.
- [0082] 여기서, 제어된 반사실적 양자 순간이동 지원 장치는 송신 단말, 수신 단말 및 제어 단말 중 어느 하나의 단말일 수 있고, 도 3은 제어된 반사실적 양자 순간이동 지원 장치가 송신 단말인 경우에 해당한다.
- [0083] 도 3을 참조하면, 송신 단말은 310 단계에서 $2N$ 개의 GHZ(Greenberger-Horne-Zeilinger)상태를 반사실적으로 생성한다.
- [0084] 320 단계에서 송신 단말은 N 개의 GHZ 상태의 임의의 서브세트를 선택하고, 선택된 서브세트의 위치를 통지한다.
- [0085] 330 단계에서 송신 단말은 측정 결과의 일관성 여부를 확인한다.
- [0086] 측정 결과의 일관성이 기 설정된 허용 가능한 임계 값까지 신뢰 가능한 경우, 송신 단말은 340 단계에서 소유한 큐비트에 대해 벨 기반 측정을 수행한다.
- [0087] 이후, 제어 단말로부터 통신이 승인되면, 350 단계에서 송신 단말은 벨 상태에 대응하는 고전적인 2비트를 사용하여 측정 결과 통지한다.
- [0089] 이하, 본 발명의 양자정보기술 통합 시스템에서 양자 실험 플랫폼에 적용될 수 있는 양자상태 단층 촬영 처리부를 설명한다.
- [0090] 양자 상태 단층 촬영(Quantum State Tomography, QST)은 미지의 양자 상태를 결정하기 위한 양자 정보 처리 작업이다. 이 작업은 동일하게 준비된 양자 시스템(identically prepared quantum system)의 앙상블(ensemble)을 측정하고, 그 상태를 다양한 추정 방법으로 추론함으로써 수행된다. 양자 상태가 측정 전, 명확한 인과 순서(고전적 궤적)가 입력된 최대 잡음 탈분극 채널을 통과할 때 양자 상태가 최대 혼합 상태로 전환되어, QST 수행이 불가능하다.
- [0091] 고전적 궤적을 통해 양자 상태를 전달하는 대신, 본 명세서의 제안 방법은 채널을 무한한 인과 순서(Indefinite Causal Order, ICO)로 설정한다. 본 명세서에서는 ICO에서 탈분극 채널을 설정하면 채널이 최대 잡음 상태에 있더라도(maximally noisy) QST를 수행할 수 있음을 보여준다. 그리고/또는, 본 명세서에서는 채널이 최대 잡음이 없을 때 선형 회귀 추정을 통해 QST에 대한 ICO의 영향을 살펴본다. 그리고/또는, 본 명세서에서는 ICO 배열에서 채널을 설정하는 것은 채널이 최대 잡음이 있을 때 유리하다는 것을 보여준다.
- [0092] 본 발명의 실시예에 따른 양자상태 단층 촬영 처리부는 추정될 양자 상태를 양자 스위치로 전송하고, 상기 양자 스위치에서 출력되는 상태에서 양자 상태 단층 촬영을 수행하고, 상기 양자 상태 단층 촬영의 출력 및 대수학에 기반하여 초기 상태를 추정할 수 있다.
- [0094] 미지의 시스템의 상태를 판별하는 양자 작업은 양자 상태 단층 촬영(QST, Quantum State Tomography)라 칭할 수 있다. QST는 두 단계로 구성될 수 있다.
- [0095] 먼저, 동일하게 준비된 양자 상태 사본에 대한 측정이 수행된다.
- [0096] 다음, 고전적인 통계 추정 방법을 사용해 양자 상태가 재구성된다. 양자 상태를 구성하는 방법은 선형 반전(methods to construct a quantum states are linear inversion, MLE), 최대 가능도 추정(maximum likelihood estimation), 베이저안 추정 방법(bayesian estimation method) 및 선형 회귀(linear regression) 등이 있을 수 있다.
- [0097] 선형 반전(Linear inversion)은 이상적인 환경을 가정하여 수행될 수 있다. 따라서, 큐비트 측정 중에 오류가 발생한 경우, 복구된 상태는 물리적 상태가 아닐 수 있다. MLE는 수치 최적화에 의해 결정된 측정 데이터 세트를 생성할 가장 높은 확률을 제공하는 밀도 행렬을 찾는다. 베이저안 방법은 베이저안 정리를 이용하여 사전 확률 분포(prior) $p(\rho)$ 에 대한 지식으로 사후 확률 분포(posterior probability distribution) $p(\rho|D)$ 를 결정

할 수 있다. 여기서 D는 측정 데이터를 의미한다.

[0098] 전통적인 양자 통신에서 양자 메시지가 일련의 통신채널 $\mathcal{N}_1$ 및 $\mathcal{N}_2$ 를 통해 전송될 때, 채널을 통해 송신되는 메시지의 순서는 채널 $\mathcal{N}_1$ 을 통과한 후에 $\mathcal{N}_2$ 또는 먼저 $\mathcal{N}_2$ 를 통과한 다음 $\mathcal{N}_1$ 을 통과하는 것으로 정의될 수 있다.

[0099] 양자 이론은 이 채널들의 중첩을 생성하여 양자 채널을 결합하는 새로운 방식을 허용할 수 있다. 이를 통해, 정보 전달 순서는 이전의 두 가지 상태에 해당하지 않는다. 즉, 양자 채널 사이의 인과 순서가 무한하다. 무한한 인과 순서의 과정은 작업 순서가 쿼텀 비트(quantum bit)로 제어되는 양자 스위치(Quantum switch)에 의할 수 있다. 그리고/또는, 두 가지 대안적 순서를 중첩하여 완전 탈분극 채널의 조합을 통해 정보가 전송될 수 있다. 양자 스위치는 양자 계측(quantum metrology), 채널 용량 향상, 양자 탈분극 채널 식별 및 양자 인터넷을 향상시키는 데 활용될 수 있다.

[0100] 본 명세서에서는 양자 상태가 측정 전에 최대 잡음이 있는 양자 탈분극 채널을 통해 전송된다는 가정하에 선형 회귀 분석을 통해 QST를 모델링한다. 그리고, 본 명세서에서는 양자 채널을 무한한 인과 순서로 설정하는 것이 QST에 미치는 영향을 살펴본다. 그리고, 본 명세서에서는 명확한(definite) 인과 순서 및 ICO로 조립된 채널을 통해 전송되는 경우 추정된 상태와 실제 상태의 부정확성(infidelity)을 비교한다. 후자의 방법은 최대 잡음이 있는 양자 탈분극 채널에 대한 QST를 지원할 수 있다.

[0101] 이하, 본 명세서에서는 먼저, 선형 회귀 방법과 양자 스위치를 통한 양자 상태 단층 촬영을 살펴보고, 명확한 인과 순서와 ICO에 따라 설정된 채널을 통해 양자 상태를 전송할 때 QST 성능을 살펴본다.

[0103] 양자 상태 단층 촬영(Quantum State Tomography)

[0104] 먼저, 미지의 양자 상태를 추정하기 위한 선형 회귀 접근법을 살펴본다.

[0105] $i = j$ 이면 1이고, 그렇지 않은 경우 0인 Kronecker의 델타 함수 δ_{ij} 를 이용할 수 있다. $\text{tr}(\cdot)$ 은 행렬의 추적을 의미하는 것으로 (1) $\text{tr}(\sigma_i) = 0$ 와 (2) $\text{tr}(\sigma_i \sigma_j) = \delta_{ij}$ 를 만족하는 Hermitian 연산자 $\{\sigma_i\}_{i=1}^{d^2-1}$ 로 지정할 수 있다. 예를 들면, 단일 큐비트의 경우(single-qubit case), $\{\sigma_i\}_{i=1}^{d^2-1}$ 는 아래 수학적 5와 같을 수 있다.

[0106] [수학적 5]

$$\left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$$

[0107]

[0108] 큐비트 밀도 연산자(operator)는 다음 수학적 6과 같이 매개변수화될 수 있다.

[0109] [수학적 6]

$$\rho = \frac{I}{d} + \sum_{i=1}^{d^2-1} r_i \sigma_i$$

[0110]

[0111] 여기서, $r_i = \text{tr}(\rho \sigma_i)$ 이고, 측정 세트 $\{\mathcal{M}_n\}_{n=1}^M$ 이 베이스(bases) $\{\sigma_i\}_{i=1}^{d^2-1}$ 하에 다음 수학적 7과 같이 매개변수화될 수 있다고 가정할 수 있다.

[0112] [수학식 7]

$$\mathcal{M}_n = \frac{I}{d} + \sum_{i=1}^{d^2-1} \psi_i^n \sigma_i$$

[0113]

[0114] 여기서, $\psi_i^n = \text{tr}(\mathcal{M}_n \sigma_i)$ 이고, $\sum_{n=1}^M \mathcal{M}_n = 1$ 이다. 이 작업에서 사용되는 측정 세트는 $\{|H\rangle\langle H|, |V\rangle\langle V|, |D\rangle\langle D|, |R\rangle\langle R|\}$ 인 스토크스 측정 세트(stokes measurement set)이다. 보른 규칙(Born's rule)에 기반하여, 동일하게 준비된 양자 시스템의 다수의 사본들이 측정된다면, $\mathcal{M}_n$ 의 측정 결과를 획득하기 위한 확률은 다음 수학식 8과 같을 수 있다.

[0115] [수학식 8]

$$\begin{aligned} p_n &= \text{tr}(\mathcal{M}_n \rho) \\ &= \text{tr}\left(\left(\frac{I}{d} + \sum_{i=1}^{d^2-1} \psi_i^n \sigma_i\right) \rho\right) \\ &= \frac{1}{d} \text{tr}(\rho) + \text{tr}\left(\sum_{i=1}^{d^2-1} \psi_i^n \sigma_i \rho\right) \\ &= \frac{1}{d} + \sum_{i=1}^{d^2-1} \psi_i^n r_i = \frac{1}{d} + \psi^{(n)T} \theta \end{aligned}$$

[0116]

[0117] 여기서, $\psi^{(n)T}$ 는 열벡터 $\psi^{(n)} = \{\psi_1^n, \dots, \psi_{d^2-1}^n\}$ 의 전치이고, $\theta = \{r_1, \dots, r_{d^2-1}\}$ 이다.

[0118] 상기 수학식 8로부터 QST에 대한 선형 회귀 형태는 다음 수학식 9와 같을 수 있다.

[0119] [수학식 9]

$$Y = X\theta$$

[0120]

[0121] 여기서, $Y = \{p_1 - \frac{1}{d}, \dots, p_M - \frac{1}{d}\}$ 이고, $X = \{\psi^{(1)T}, \dots, \psi^{(M)T}\}^T$ 이다.

[0122] 각 $\{\mathcal{M}_n\}_{n=1}^{d^2-1}$ 에 대해 상태 ρ 에서 양자 시스템을 N번 측정하는 것을 가정할 수 있다. 측정 결과 $\mathcal{M}_n$ 을 획득하기 위한 확률은 다음 수학식 10에 의해 추정될 수 있다.

[0123] [수학식 10]

$$\hat{p}_n = \frac{f_n}{N}$$

[0124]

[0125] 여기서, f_n 는 추정 오류 $e_n = \hat{p}_n - p_n$ 를 갖는 관찰된 주파수들을 나타낸다. 다음, 상기 수학식 9에서 선형 회귀 방정식은 다음 수학식 11과 같을 수 있다.

[0126] [수학식 11]

$$Y = X\theta + e$$

[0127]

[0128] 여기서, $Y = \{\hat{p}_1 - \frac{1}{d}, \dots, \hat{p}_M - \frac{1}{d}\}$ 이고, $e = \{e_1, \dots, e_M\}$ 이다. 큰 N의 경우, $\{e_n\}_{n=1}^M$ 은 평균 0과 변

화량 $\frac{p_n - p_n^2}{N}$ 를 갖는 정규 분포에 대한 분포로 수렴될 수 있다. 많은 측정이 수행된다면, 큐비트 상태에 대한 측정은 더 정확해질 수 있다. 상기 수학식 11에서 선형 회귀 문제에 대한 해결책은 다음 수학식 12를 최소화하는 θ 일 수 있다.

[0129] [수학식 12]

$$\begin{aligned}\hat{\theta} &= \arg \max_{\theta} (Y - X\theta)^T (Y - X\theta) \\ &= (X^T X)^{-1} X^T Y.\end{aligned}$$

[0130] 추정 세트 $\{\mathcal{M}_n\}_{n=1}^M$ 이 정보적으로 완전하거나 넘쳐서 $(X^T X)$ 역을 가지는 것을 가정할 수 있다. 추정값 $\hat{\theta}$ 는 평균 제곱 오차(mean squared error)를 갖는 평향되지 않는 추정값이고, 점근적으로, 다음 수학식 13과 같을 수 있다.

[0131] [수학식 13]

$$MSE_{\hat{\theta}} = \text{tr} \left((X^T X)^{-1} X^T P X (X^T X)^{-1} \right)$$

[0132] 여기서, $P = \frac{1}{N} \text{diag} \{p_1 - p_1^2, \dots, p_M - p_M^2\}$ 이다.

[0133] 양자 탈분극 채널(Quantum Depolarizing Channel)

[0134] 양자 정보는 양자 채널을 통해 전송될 수 있다. 양자 채널은 밀도 연산자에 대한 맵을 보존하는 완전한 양의 추적으로서 수학적으로 정의될 수 있다. 채널을 통해 전송되는 동안, 큐비트는 확률 $(1-q)$ 를 갖는 완전히 혼합된 상태로 진화(evolution)하고, 확률 q 로 그대로 유지될 수 있다. 이러한 종류의 양자 채널을 양자 탈분극 채널 $\mathcal{N}(\rho)$ 이라 칭할 수 있다. 큐비트의 진화 ρ 는 다음 수학식 14와 같이 정의된다.

[0135] [수학식 14]

$$\mathcal{N}(\rho) = (1-q) \frac{I}{d} + q\rho$$

[0136] 양자 스위치 (Quantum Switch)

[0137] 상술한 바와 같이, 두 개의 양자 채널을 통해 전송되는 양자 시스템은 명확한 인과 순서로 진화하고, 두 번째 채널은 첫 번째 채널의 출력에 작용한다. 양자 시스템은 ICO에서도 진화할 수 있기 때문에 어떤 과정이 다른 과정보다 먼저 일어나는지 결정할 수 없다. 이것은 양자 스위치 때문에 가능하다. 양자 스위치는 양자 채널을 결합하고, 제어 큐비트라고 하는 큐비트 ρ_c 에 의해 상대적인 순서를 제어할 수 있다. 제어 큐비트가 $\rho_c = |0\rangle\langle 0|$ 상태에 있는 경우, 양자 스위치는 $\mathcal{N}_1 \rightarrow \mathcal{N}_2$ 순서에 따라 양자 시스템을 지나갈 것이다. 제어 큐비트가 $|1\rangle\langle 1|$ 상태에 있다면, 양자 상태는 $\mathcal{N}_2 \rightarrow \mathcal{N}_1$ 순서에 따라 양자 채널을 지나간다. 제어 큐비트가 $|+\rangle\langle +|$ 와 같이 $|0\rangle$ 와 $|1\rangle$ 의 중첩에 있는 경우, 양자 스위치는 채널을 $\mathcal{N}_1 \rightarrow \mathcal{N}_2$ 와 $\mathcal{N}_2 \rightarrow \mathcal{N}_1$ 순서의 중첩에 둘 수 있다. 양자 스위치의 결과로서 양자 채널의 Kraus 연산자는 다음 수학식 15와 같이 정의될 수 있다.

[0138] [수학식 15]

$$W_{ij} = K_i^{(2)} K_j^{(1)} \otimes |0\rangle\langle 0|^c + K_j^{(1)} K_i^{(2)} \otimes |1\rangle\langle 1|^c$$

[0145] 여기서, 채널 $\mathcal{N}_1$ 와 $\mathcal{N}_2$ 의 Kraus 연산자는 각각 $K_i^{(1)}$ 와 $K_i^{(2)}$ 로 나타낼 수 있다.

[0146] 하나의 큐비트 시스템에 대한 양자 스위치는 다음 수학적 식 16과 같이 주어질 수 있다.

[0147] [수학적 식 16]

$$\mathcal{S}(\mathcal{N}_1, \mathcal{N}_2)(\rho \otimes \rho_c) = \sum W_{ij}(\rho \otimes \rho_c)W_{ij}^\dagger.$$

[0150] 단층 촬영 방법, 시뮬레이션 및 결과

[0151] 추론할 양자 상태 ρ 가 고전적인 궤적에서 잡음이 있는 탈분극 채널을 통해 측정 시스템으로 전송된다고 가정할 수 있다. 채널이 최대 잡음인 경우, 예를 들면 $q = 0$ 일 때, 수학적 식 10으로부터 큐비트는 ρ 에 종속하지 않는 다음 수학적 식 17의 최대 혼합 상태로 변환될 수 있다.

[0152] [수학적 식 17]

$$\mathcal{N}(\rho) = \frac{I}{d}$$

[0154] 결론적으로, $\mathcal{N}(\rho)$ 에서 QST가 수행된다면, ρ 를 재구성하는 것은 불가능하다.

[0155] 제어 큐비트 $\rho_c = |c\rangle\langle c|$ 를(여기서, $|c\rangle = \sqrt{a}|0\rangle + \sqrt{\bar{a}}|1\rangle$) 갖는 무한한 인과 순서에서 채널이 설정된다면, 채널의 출력은 다음 수학적 식 18과 같을 수 있다.

[0156] [수학적 식 18]

$$\mathcal{P}(\mathcal{N}_1, \mathcal{N}_2)(\rho, \rho_c) = \bar{q}^2 \left[(a|0\rangle\langle 0| + \bar{a}|1\rangle\langle 1|) \otimes \frac{I}{d} + \sqrt{a\bar{a}}(|0\rangle\langle 1| + |1\rangle\langle 0|) \otimes \frac{\rho}{d^2} \right] + 2q\bar{q} \left(\rho_c \otimes \frac{I}{d} \right) + q^2 \rho_c \otimes \rho$$

[0157]

[0158] $\{|+\rangle, |-\rangle\}$ 베이스(basis)에서 제어 큐비트의 측정은 채널의 출력을 다음 수학적 식 19와 같이 변환할 수 있다.

[0159] [수학적 식 19]

$$\rho^{QS} = \begin{cases} \rho_{|+\rangle}^{QS} = \bar{q}^2 \left(\frac{I}{2d} + \sqrt{a\bar{a}} \frac{\rho}{d^2} \right) + 2q\bar{q} \frac{I}{d} + q^2 \rho, & \text{pr}_{|+\rangle} = \bar{q} \frac{d + \sqrt{a\bar{a}}}{d^2} + \frac{4q\bar{q}}{d} + q^2. \\ \rho_{|-\rangle}^{QS} = \bar{q}^2 \left(\frac{I}{2d} - \sqrt{a\bar{a}} \frac{\rho}{d^2} \right) & , \text{pr}_{|-\rangle} = 1 - \text{pr}_{|+\rangle} \end{cases}$$

[0160]

[0161] 여기서, $\text{pr}_{|+\rangle}$ 와 $\text{pr}_{|-\rangle}$ 는 각각 $|+\rangle$ 와 $|-\rangle$ 에서 측정 결과를 획득하는 확률을 나타낼 수 있다. 채널이 최대로 잡음이 있는 경우, 수학적 식 19로부터, ρ^{QS} 에 대해 QST를 수행한다면, ρ^{QS} 는 상태 ρ 를 재구성할 수 있는 것을 의미하는 ρ 에 의존할 수 있다.

[0162] ρ^{QS} 를 측정한다면, ρ 가 아닌 ρ^{QS} 의 추정을 얻을 것이다.

[0163] 양자 상태의 확률이 온전히 남아 있는지 여부는 ρ 를 다음 수학적 식 20과 같이 복구할 수 있는 수학적 식 19로부터 양자 처리 단층 촬영(quantum process tomography)에 의해 결정될 수 있다.

[0164] [수학식 20]

$$\hat{\rho} = \begin{cases} \left(\hat{\rho}^{QS} \text{pr}_{|+\rangle} - \frac{\bar{q}^2}{2d} I - \frac{2q\bar{q}}{d} I \right) / \left(\frac{\bar{q}^2 \sqrt{a\bar{a}}}{d^2} + q^2 \right) & , \text{for } \rho_{|+\rangle}^{QS} \\ \left(\frac{\bar{q}^2}{2d} I - \hat{\rho}^{QS} \text{pr}_{|-\rangle} \right) / \left(\frac{\bar{q}^2 \sqrt{a\bar{a}}}{d^2} \right) & , \text{for } \rho_{|-\rangle}^{QS} \end{cases}$$

[0165] ρ^{QS} , 상에 수학식 20이 적용되는 경우, $\hat{\rho}$ 가 비물리적 행렬인 몇가지 경우들이 있을 수 있다.

[0166] 이러한 이유로, $\hat{\rho}$ 를 물리적 행렬 공간에 투영할 수 있고, 단위 트레이스와 양의 반정의 행렬들의 공간으로 표현될 수 있다. 단순 투영 알고리즘은 채택될 수 있으며, 이것의 아이디어는 밀도 행렬의 모든 고윳값들을 양의 값들 그리고 이들의 합으로 변환하는 것일 수 있다.

[0167] <MSE 분석(MSE analysis)>

[0168] 수학식 19에서의 양자 상태가 측정된다면, 상태 $\rho_{|+\rangle}^{QS}$ 에 대한 $\mathcal{M}_n$ 의 측정 결과를 획득하기 위한 확률은 다음 수학식 21과 같이 정의될 수 있다.

[0169] [수학식 21]

$$\begin{aligned} \hat{p}_n^{QS} &= \text{tr} \left(\mathcal{M}_n \rho_{|+\rangle}^{QS} \right) \\ &= \frac{1}{\text{pr}_{|+\rangle}} \left[\bar{q}^2 \left(\frac{1}{2d} + \frac{\sqrt{a\bar{a}}}{d^2} p_n \right) + \frac{2q\bar{q}}{d} + q^2 p_n \right] \end{aligned}$$

[0170] 상태 $\rho_{|-\rangle}^{QS}$ 의 경우, 확률은 다음 수학식 22와 같이 정의될 수 있다.

[0171] [수학식 22]

$$\begin{aligned} \hat{p}_n^{QS} &= \text{tr} \left(\mathcal{M}_n \rho_{|-\rangle}^{QS} \right) \\ &= \frac{1}{\text{pr}_{|-\rangle}} \left[\bar{q}^2 \left(\frac{1}{2d} - \frac{\sqrt{a\bar{a}}}{d^2} p_n \right) \right] \end{aligned}$$

[0172] 최대 노이즈 채널($q=0$)의 경우, $\hat{p}_n^{QS}$ 는 다음 수학식 23와 같을 수 있다.

[0173] [수학식 23]

$$\hat{p}_n^{QS} = \begin{cases} \frac{1}{\text{pr}_{|+\rangle}} \left(\frac{1}{2d} + \frac{\sqrt{a\bar{a}}}{d^2} p_n \right) & , \text{for } \rho_{|+\rangle}^{QS} \\ \frac{1}{\text{pr}_{|-\rangle}} \left(\frac{1}{2d} - \frac{\sqrt{a\bar{a}}}{d^2} p_n \right) & , \text{for } \rho_{|-\rangle}^{QS} \end{cases}$$

[0174] 여기서, 제어 큐비트가 상태 $|-\rangle$ 에 해당하는 경우, 즉 $\text{MSE}_{\theta, |-\rangle} < \text{MSE}_{\theta, |+\rangle}$ 인 경우, 더 나은 결과는 얻어질 수 있다.

[0175] 수학식 13으로부터, X는 제어 큐비트 측정 후 획득된 양쪽 상태에 대한 동일한 값을 얻을 수 있다. 그러므로, P에 의해 야기된 차이점을 확인해야할 필요가 있다.

[0176] 모순을 가정하기 위해, $\text{MSE}_{\theta, |-\rangle} > \text{MSE}_{\theta, |+\rangle}$ 는 다음 수학식 24로부터 수학식 25의 과정을 거쳐 수학식 26으로 표현될 수 있다.

[0181] [수학식 24]

$$[0182] \quad \text{MSE}_{\theta, |-} - \text{MSE}_{\theta, |+} > 0$$

[0183] [수학식 25]

$$[0184] \quad (\hat{p}_{n,|-} - \hat{p}_{n,|-})^2 - (\hat{p}_{n,|+} - \hat{p}_{n,|+})^2 > 0$$

[0185] [수학식 26]

$$[0186] \quad A - B - C + D - E > 0$$

[0188] 여기서,

$$A = \frac{1}{2d} \left(\frac{1}{\text{pr}_{|-}} - \frac{1}{\text{pr}_{|+}} \right) \quad \text{이고}, \quad B = \frac{\sqrt{a\bar{a}}}{d^2} p_n \left(\frac{1}{\text{pr}_{|-}} + \frac{1}{\text{pr}_{|+}} \right) \quad \text{이며},$$

$$C = \frac{1}{4d^2} \left(\frac{1}{\text{pr}_{|-}^2} - \frac{1}{\text{pr}_{|+}^2} \right) \quad \text{이고}, \quad D = \frac{\sqrt{a\bar{a}}}{d^3} p_n \left(\frac{1}{\text{pr}_{|-}^2} - \frac{1}{\text{pr}_{|+}^2} \right) \quad \text{이며},$$

$$E = \frac{a\bar{a}}{d^4} p_n^2 \left(\frac{1}{\text{pr}_{|-}^2} - \frac{1}{\text{pr}_{|+}^2} \right) \quad \text{이다.}$$

[0189] 여기서, 수학식 26은 $A + D < B + C + E$ 로 표현될 수 있고, $A + D < B + C + E$ 은 모순이다. 그러므로, $\text{MSE}_{\theta, |-} < \text{MSE}_{\theta, |+}$ 여야 할 수 있다.

[0190] 수학식 17로부터 양자 상태가 고전(classical) 배열을 통해 전송되는 경우, $\mathcal{M}_n$ 의 측정 결과를 획득하기 위한 확률은 $\hat{p}_n = \frac{1}{d}$ 이고, 이에 따라 $\text{MSE}_{\theta, |-}$ 와 $\text{MSE}_{\theta, |+}$ 보다 더 큰 MSE는 주어질 것이다.

[0191] <수치 시뮬레이션(Numerical Simulation)>

[0192] 이하에서는, 상술한 체계를 사용하여 하나의 큐비트 시스템에서 수치 시뮬레이션을 수행한다. 순수 상태와 혼합 상태에서 QST를 수행하여 두 가지 상태 모두에서 체계가 잘 작동하는지 확인한다.

[0193] 도 4는 큐비트 전송에서 양자 스위치(410)를 채택함으로써, 최대 잡음이 있는 양자 탈분극 채널에서 QST를 수행하기 위한 메커니즘을 설명하는 도면이다.

[0194] 도 4를 참조하면, 시뮬레이션 시 구성되는 일실시에 따른 단층 촬영 장치(400)는 양자 스위치(Quantum Switch)(410)와, 제어 큐비트를 측정하는 측정(Control Qubit Measurement) 장치(420)와, 양자 상태 단층 촬영(Quantum State Tomography) 장치(430)를 포함할 수 있다.

[0195] Haar 측정(measure)에 따라, 그리고 혼합 상태들을 위한 힐베르트-슈미트(Hilbert-Schmidt) 측정(measure) 또는 Bures 측정(measure)에 따라 균일하게 분포된 5×10^3 개의 임의 양자 상태들이 생성될 수 있다. 측정 전에 고전적 궤도에서 조립된 최대 잡음이 있는 탈분극 채널 및 ICO에서 큐비트 전송을 모델링할 수 있다. 6×10^3 측정들은 각 큐비트 상에서 각 $\{\mathcal{M}_n\}_{n=1}^{d^2-1}$ 마다 수행될 수 있다. 실제 상태와 추정치 얼마나 가까운지 정량화하기 위해, 양쪽 상태 $F(\rho, \hat{\rho}) = \text{tr}(\sqrt{\sqrt{\rho}\hat{\rho}\sqrt{\rho}})$ 모두의 정확도(fidelity)가 계산될 수 있다.

[0196] 다음, 5×10^3 개의 양자 상태들의 평균 log 정확도 $\log_{10}(1 - F(\rho, \hat{\rho}))$ 는 계산될 수 있다. 상태들이 유한한 인과 순서 그리고 ICO에서 전송되는 경우, 이러한 추정을 갖는 실제 순수 상태들의 Log 부정확도(infidelity)는 도 5와 같이 나타낼 수 있다.

- [0197] 도 5는 순수 상태들 (a)과 혼합 상태들 (b)에 대한 재구성 상태 $\hat{\rho}$ 와 실제 상태 ρ 의 Log 부정확도 (infidelity)를 나타낸다.
- [0198] 실제 상태들이 ICO 배열에서 놓여진 채널을 통해 전송되는 경우, log 부정확도(infidelity)는 각 $|+\rangle$ 와 $|-\rangle$ 에서의 측정 결과에 대해 빨간 색과 녹색 선에 의해 표시될 수 있다. 또한, 추정된 상태의 평균 정확도는 다음 수학적 식 27과 같이 계산될 수 있다.
- [0199] [수학적 식 27]
- [0200]
$$F_{av} = \text{pr}_{|+\rangle} F_{|+\rangle} + \text{pr}_{|-\rangle} F_{|-\rangle}$$
- [0201] 여기서, $\text{pr}_{|+\rangle}$, $\text{pr}_{|-\rangle}$, $F_{|+\rangle}$ 및 $F_{|-\rangle}$ 는 제어 큐비트의 측정이 $|+\rangle$ 와 $|-\rangle$ 에 대응하는 경우, 추정된 상태의 확률과 정확도일 수 있다.
- [0202] 도 5로부터, 최대 잡음이 있는 양자 탈분극 채널에 대해, ICO 배열이 순수 상태 및 혼합 상태 양쪽 모두에 대한 QST 추정 성능에 도움이 되는 것을 확인할 수 있다. 측정 결과 $|-\rangle$ 에 해당하는 상태들 상에 QST는 이전에 설명된 MSE 분석과 일치하는 $|+\rangle$ 에 해당하는 상태들보다 더 좋은 추정을 획득할 수 있다.
- [0204] 예를 들어, 도 6의 일실시예에 따른 단층 촬영 장치(600)는 상술한 동작을 수행할 수 있다. 예를 들어, 단층 촬영 장치(600)의 양자 스위치부(610)를 통과한 출력은 수학적 식 18과 같을 수 있다. 그리고/또는, 단층 촬영 장치(600)의 양자 스위치부(610)는 $\{|+\rangle, |-\rangle\}$ 베이스(basis)에서의 제어 큐비트에서 채널의 출력을 수학적 식 19와 같이 변환할 수 있다. 그리고/또는, 단층 촬영 장치(600)의 단층 촬영부(620) 및/또는 추정부(630)는 상기의 양자 상태 단층 촬영에 대한 설명과 같이 선형 회귀 접근법에 기반하여 양자 상태를 추정할 수 있다. 예를 들어, 단층 촬영 장치(600)의 단층 촬영부(620) 및/또는 추정부(630)는 수학적 식 5 내지 수학적 식 13의 연산을 수행할 수 있다. 그리고/또는, 단층 촬영 장치(600)의 단층 촬영부(620) 및/또는 추정부(630)는 수학적 식 19에 기반하여 ρ 를 재구성할 수도 있다.
- [0205] 그리고/또는, 단층 촬영 장치(600)의 단층 촬영부(620) 및/또는 추정부(630)는 수학적 식 16에 의해 ρ 에 또는 $\hat{\rho}$ 를 결정 및/또는 추정할 수 있다.
- [0206] 도 6을 참조하여 설명한 단층 촬영 장치의 동작은 상술한 방식에 한하지 않으며, 다양한 방식으로 본 명세서에서 설명된 동작들을 수행할 수 있다. 또한, 단층 촬영 장치는 상기 도 6을 참조하여 설명한 단층 촬영 장치의 동작 이외에도 본 명세서에서 설명된 모든 또는 일부 동작들을 수행할 수 있다.
- [0207] 도 6의 단층 촬영 장치는 도 7의 양자 상태 단층 촬영 처리부(2031)에 적용될 수 있다.
- [0208] 본 명세서에서는 최대 잡음이 있는 탈분극 채널에서의 QST를 살펴보았다. 본 명세서에서는 최대 잡음 채널에서 QST가 가능하도록 양자 스위치(quantum switch)를 적용하였다. 본 명세서에서 설명한 바와 같이, 양자 전환 배열로 큐비트를 전송하는 것이 고전적인 케이블을 통해 전송하는 것보다 더 정확한 양자 상태 추정을 제공한다. 다시 말해, 본 발명은 최대 잡음이 있는 탈분극 양자 채널에서 정확한 양자 상태 단층 촬영을 수행할 수 있다.
- [0210] 도 6은 본 발명의 일실시예에 따른 단층 촬영 장치의 블록도이다.
- [0211] 도 6을 참조하면, 본 발명의 일실시예에 따른 단층 촬영 장치(600)는 제어 큐비트에 의해 제어되고 추정될 양자 상태를 수신하는 양자 스위치부(610)와, 양자 스위치부(610)에서 출력되는 상태에 양자 상태 단층 촬영을 수행하는 단층 촬영부(620)와, 단층 촬영부(620)의 출력 및 대수학에 기반하여 초기 상태를 추정하는 추정부(630)를 포함하며, 최대 잡음 채널에서도 양자 상태 촬영이 수행될 수 있다.
- [0212] 그리고/또는, 양자 스위치부(610)는 양자 채널을 결합할 수 있다.
- [0213] 그리고/또는, 단층 촬영은 선형 회귀 추정에 기반할 수 있다.

- [0214] 그리고/또는, 최대 잡음 채널은 무한 인과 순서(Indefinite Causal Order, ICO)로 설정될 수 있다.
- [0215] 그리고/또는, 최대 잡음 채널은 양자 탈분극 채널일 수 있다.
- [0216] 다른 일실시예에 따라, 단층 촬영 장치(600)는 추정될 양자 상태를 양자 스위치로 전송하고, 양자 스위치에서 출력되는 상태에서 양자 상태 단층 촬영을 수행하며, 양자 스위치에서 출력되는 상태의 예측에서 대수학을 수행하여 초기 상태를 추정함에 따라 최대 잡음 탈분극 양자 채널에서 양자 상태 단층 촬영 정확도를 향상시킬 수 있다.
- [0217] 다른 일실시예에 따라, 단층 촬영 장치(600)는 추정될 양자 상태를 양자 스위치로 전송하고, 양자 스위치에서 출력되는 상태에서 양자 상태 단층 촬영을 수행하며, 양자 스위치에서 출력되는 상태의 예측에서 대수학을 수행하여 초기 상태를 추정함으로써, 채널 잡음이 최대인 경우에도 양자 상태 단층 촬영을 수행할 수 있다.
- [0218] 그리고/또는, 양자 상태는 최대 잡음 탈분극 양자 채널로 전송되면 최대한으로 혼합된 상태로 변환하면서 양자 상태 단층 촬영을 수행할 수 없게 된다. 채널 잡음이 최대인 경우에도 일실시 예에 따른 양자 상태 단층 촬영 장치는 먼저, 추정될 양자 상태를 양자 스위치로 전송하고, 양자 스위치에서 출력되는 상태에서 양자 상태 단층 촬영을 수행하며, 양자 스위치에서 출력되는 상태의 예측에서 대수학을 수행하여 초기 상태를 추정할 수 있다.
- [0219] 도 6을 참조하여 설명한 단층 촬영 장치의 동작은 이에 한정되지 않으며, 이외 본 명세서에서 설명된 모든 또는 일부 동작들이 단층 촬영 장치에 의해 수행될 수 있다.
- [0221] 도 7은 본 발명의 실시예에 따른 양자정보기술 통합 시스템을 나타내는 도면이다.
- [0222] 도 7을 참조하면, 양자 통신 플랫폼(2010), 양자 컴퓨팅 플랫폼(2020), 양자 관측 및 분석 플랫폼(2030), 플랫폼 제어부(2040) 및 플랫폼 인터페이스부(2050)를 포함한다.
- [0223] 양자 통신 플랫폼(2010)은 양자통신 및 양자정보통신과 관련된 요소 기술의 구현 및 실험을 제공하는 플랫폼이다.
- [0224] 양자 통신 플랫폼(2010)은 양자 키 분배(quantum key distribution: QKD)를 통해 보안된 통신을 수행하는 양자 키 분배 처리부(2011), 채널에 입자가 존재하지 않는 무-입자(particle-free) 정보전송과 새로운 형태의 전 이중(full-duplex) 정보전송 및 익명-원격계산(blind tele-computation) 등을 수행하는 반사실 양자 통신 처리부(2013), 차세대이동통신에 양자 통신을 적용하는 경우 무선자원 관리를 수행하는 무선 자원 관리 처리부(2015) 및 네트워크 간섭 제어를 수행하는 네트워크 간섭 제어 처리부(2017)를 포함할 수 있다. 예를 들어, 반사실 양자통신 처리부(2013)는 제1 단말(Alice), 제2 단말(Bob) 및 제3 단말(Charlie) 중 적어도 어느 하나의 역할을 수행할 수 있다.
- [0225] 양자 컴퓨팅 플랫폼(2020)은 양자 알고리즘을 기반으로 기하급수적으로 빠른 병렬계산이 가능한 양자컴퓨터의 실용화를 위한 요소 기술의 구현 및 실험을 제공하는 플랫폼이다.
- [0226] 양자 컴퓨팅 플랫폼(2020)은 잡음중규모양자(noisy intermediate-scale quantum: NISQ) 장치를 위해 특별히 설계된 변형 양자알고리즘(variational quantum algorithm: VQA)을 제공하는 변형 양자 알고리즘 처리부(2021), Grover 검색 알고리즘 또는 양자 카운팅 알고리즘과 같은 양자 검색 알고리즘(quantum search algorithm: QSA)을 제공하는 양자 검색 알고리즘 처리부(2023) 및 다체(multi-body) Hamiltonian의 양자강화학습(quantum reinforcement learning)과 같은 양자머신러닝(quantum machine learning: QML) 기술을 제공하는 양자 머신 러닝 처리부(2025)를 포함할 수 있다.
- [0227] 양자 관측 및 분석 플랫폼(2030)은 양자 측정 및 양자 시뮬레이션을 지원하고, 양자 결맞음(coherence) 및 얽힘(entanglement)과 같은 실제 입자의 양자특성을 직접 활용하기 때문에 고전 컴퓨터에서 모의실험하기 어려운 문제를 해결하기 위한 플랫폼이다.
- [0228] 양자 관측 및 분석 플랫폼(2030)은 양자 상태 단층 촬영을 제공하는 양자 상태 단층 촬영 처리부(2031), 양자 상태 측정을 지원하는 양자 상태 측정 처리부(2033), 큐비트 측정 및 실험을 위한 양자 상관 측정을 지원하는 양자 상관 측정 처리부(2035) 및 모의실험을 위한 텐서 네트워크 및 Hamiltonian 기반 양자시뮬레이션을 지원하는 텐서 네트워크 실험 처리부(2037)를 포함한다.
- [0229] 플랫폼 제어부(240)은 양자 통신 플랫폼(2010), 양자 컴퓨팅 플랫폼(2020) 및 양자 관측 및 분석 플랫폼(2030)

에서 수행된 내역 및 측정 결과를 저장하고, 어느 하나의 플랫폼에서 다른 플랫폼의 구성요소의 사용이 필요할 때 이를 연결해 주는 동작을 수행할 수 있다.

[0230] 예를 들어, 양자 통신 플랫폼(2010)의 반사실 양자 통신 처리부(2013)에서 벨 측정이 필요한 경우 벨 측정은 양자 관측 및 분석 플랫폼(2030)의 양자 상태 측정 처리부(2033) 또는 양자 상관 측정 처리부(2035)에서 수행될 수도 있다.

[0231] 플랫폼 인터페이스부(2050)는 사용자 또는 실험자가 각 플랫폼에 접속할 수 있는 컴퓨터 장치일 수 있다. 예를 들어, 사용자는 플랫폼 인터페이스부(2050)를 통해 양자 관측 및 분석 플랫폼(2030)에 접속하여 원하는 양자 시뮬레이션을 실행할 수 있다.

[0233] 양자정보기술은 통신, 알고리즘 및 시뮬레이션 기술 분야와 융합되어 네트워크 보안, 무선자 원 관리, 채널추정, 네트워크 간섭관리 등 차세대이동통신의 한계를 극복하기 위한 방향으로 지속적으로 연구가 진행되고 있다. 따라서, 양자 통신 플랫폼(2010), 양자 컴퓨팅 플랫폼(2020) 및 양자 관측 및 분석 플랫폼(2030) 각각에 포함되는 구성요소는 각 기술의 발전 및 출현에 따라 대체되거나 개량될 수 있다.

[0234] 예를 들어, 양자 키 분배 처리부(2011)는 차세대이동통신 시스템의 보안계층에 융합되기 위한 기술을 제공하기 위하여 개량될 수 있다.

[0235] 예를 들어, 지능형 네트워크 기능을 요구하는 차세대이동통신 시스템의 간섭 관리에 활용하기 위하여 양자 통신 플랫폼(2010)의 각 구성요소는 개량될 수 있다.

[0237] 이상에서 설명된 장치는 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPA(field programmable array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[0239] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0240]

[0241] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태

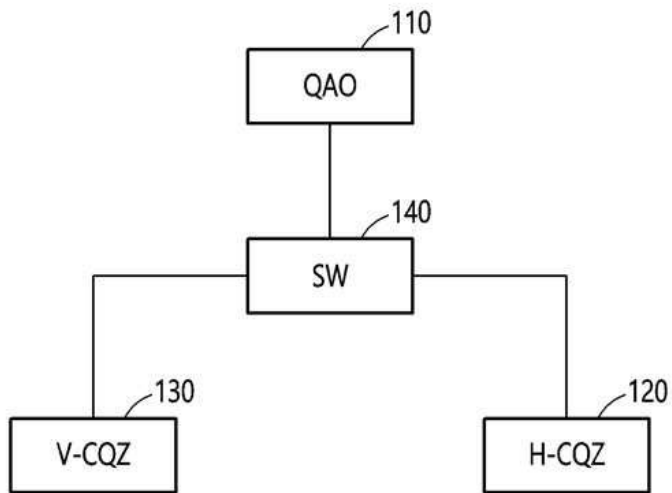
로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

[0242]

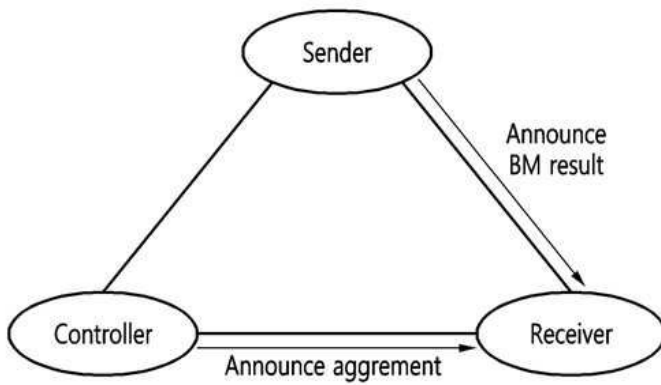
[0243] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

도면

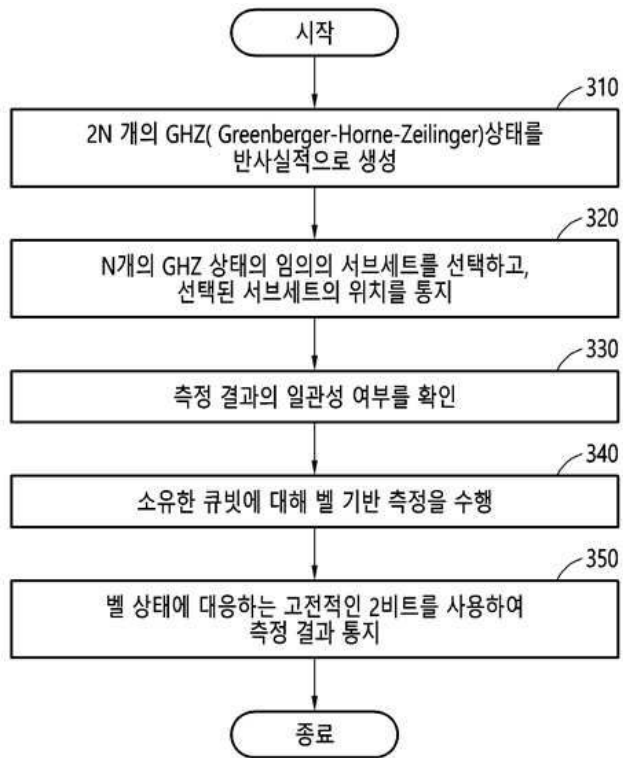
도면1



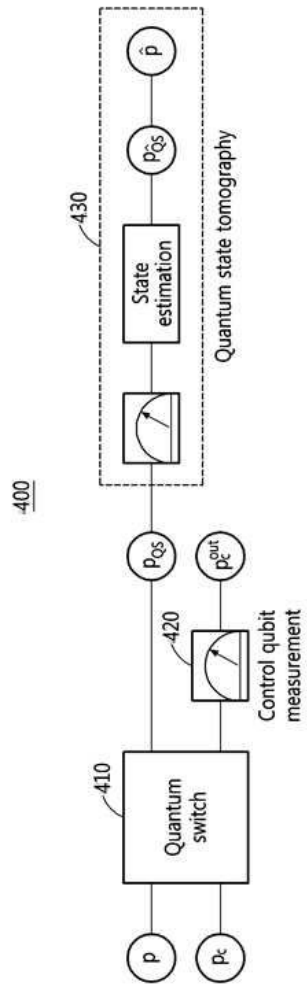
도면2



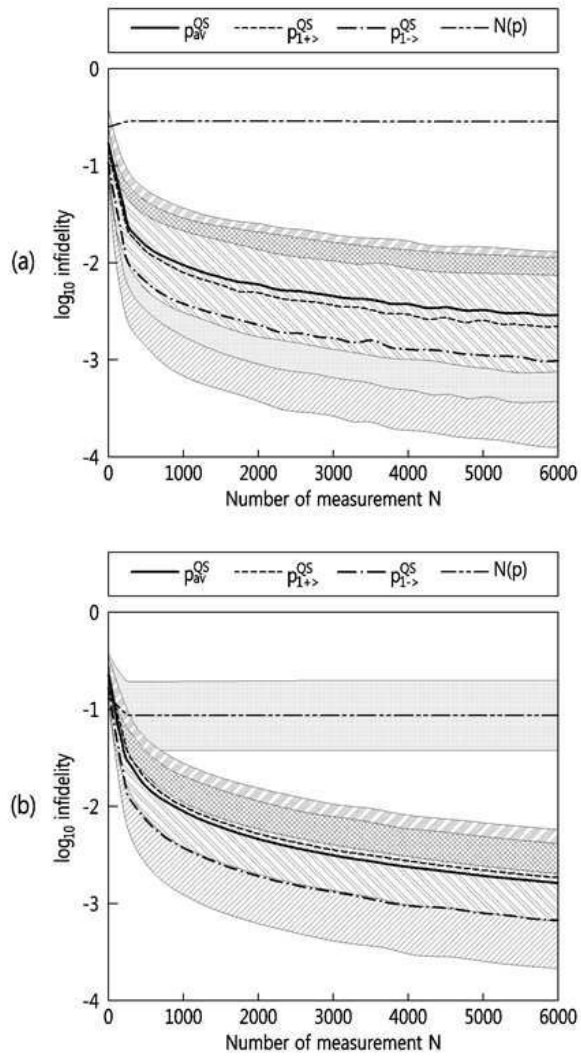
도면3



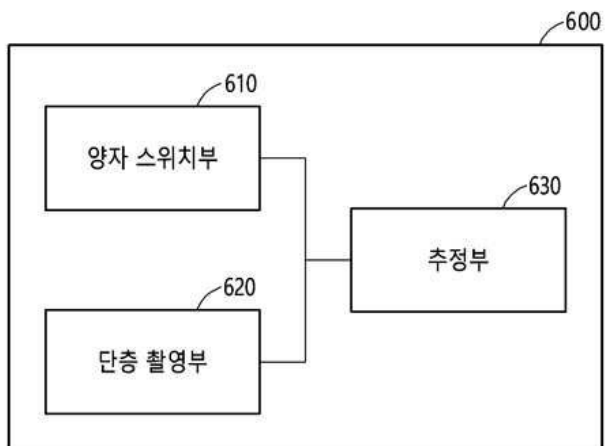
도면4



도면5



도면6



도면7

