(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년05월26일
(11) 등록번호 10-1740384
(24) 등록일자 2017년05월22일

(51) 국제특허분류(Int. Cl.)
G06F 15/173 (2006.01) *G06F 13/14* (2006.01)
G06N 99/00 (2010.01) *H04B 10/70* (2013.01)
(52) CPC특허분류
G06F 15/173 (2013.01)
G06F 13/14 (2013.01)
(21) 출원번호 10-2016-0063045
(22) 출원일자 2016년05월23일
심사청구일자 2016년05월23일
(56) 선행기술조사문헌
KR1020080056273 A
KR1020050100074 A

(73) 특허권자
경희대학교 산학협력단
경기도 용인시 기흥구 덕영대로 1732 (서천동, 경희대학교 국제캠퍼스내)
(72) 발명자
신현동
경기도 수원시 영통구 청명북로 81, 404동 901호 (영통동, 청명마을주공아파트)
사드
경기도 용인시 기흥구 덕영대로 1732, 경희대학교 전자정보관 559호(서천동)
정영민
경기도 수원시 영통구 매영로415번길 50 , 스타빌 305호(영통동)
(74) 대리인
최영한, 지덕규

전체 청구항 수 : 총 25 항 심사관 : 홍경아

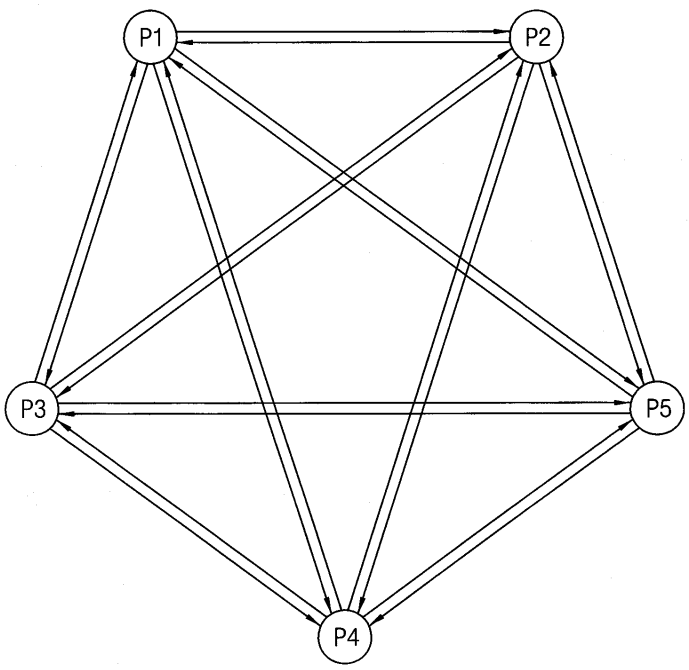
(54) 발명의 명칭 **양자 추첨 방법, 이를 이용한 양자 통신 방법 및 이를 수행하는 양자 통신 시스템**

(57) 요 약

양자 추첨 방법은 N개(N은 3 이상의 자연수)의 통신 주체들 각각이 본인을 제외한 다른 N-1개의 통신 주체들에게 각각 전송하기 위한 N-1개의 큐빗 집합들을 생성하는 단계, 상기 N개의 통신 주체들 각각이 상기 N-1개의 큐빗 집합들을 제1 베이시스 및 제2 베이시스를 이용하여 인코딩하는 단계, 상기 N개의 통신 주체들 각각이 인코딩된

(뒷면에 계속)

대 표 도 - 도1



상기 N-1개의 큐빗 집합들을 상기 N-1개의 통신 주체들에게 각각 전송하는 단계, 상기 N개의 통신 주체들 각각이 상기 N-1개의 통신 주체들로부터 입력 받은 N-1개의 큐빗 집합들을 상기 제1 베이시스 및 상기 제2 베이시스를 이용하여 측정하는 단계, 상기 N개의 통신 주체들 각각이 상기 N-1개의 큐빗 집합들이 인코딩될 때 이용된 베이시스를 각각 예측하여 N-1개의 예측 베이시스를 상기 N-1개의 통신 주체들에 각각 전송하는 단계 및 상기 N개의 통신 주체들 각각이 상기 N-1개의 통신 주체들로부터 입력 받은 상기 예측 베이시스들이 상기 N-1개의 큐빗 집합들의 인코딩 시에 이용된 인코딩 베이시스들과 일치하는지를 판단하여 상기 예측 베이시스와 상기 인코딩 베이시스의 일치 여부를 상기 N-1개의 통신 주체들에게 전송하는 단계를 포함한다.

(52) CPC특허분류
G06N 99/002 (2013.01)
H04B 10/70 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 R0190-15-2030
부처명 미래창조과학부
연구관리전문기관 한국연구재단
연구사업명 정보통신방송연구개발사업
연구과제명 양자암호통신망 구축을 통한 신뢰성 검증기술 및 QKD 고도화를 위한 핵심 요소기술 개발
기 여 율 1/1
주관기관 고려대학교 산학협력단
연구기간 2015.06.01 ~ 2016.05.31
공지예외적용 : 있음

명 세 서

청구범위

청구항 1

N개(N은 3 이상의 자연수)의 통신 주체들 각각이 본인을 제외한 다른 N-1개의 통신 주체들에게 각각 전송하기 위한 N-1개의 큐빗 집합들을 생성하는 단계;

상기 N개의 통신 주체들 각각이 상기 N-1개의 큐빗 집합들을 제1 베이시스 및 제2 베이시스를 이용하여 인코딩하는 단계;

상기 N개의 통신 주체들 각각이 인코딩된 상기 N-1개의 큐빗 집합들을 상기 N-1개의 통신 주체들에게 각각 전송하는 단계;

상기 N개의 통신 주체들 각각이 상기 N-1개의 통신 주체들로부터 입력 받은 N-1개의 큐빗 집합들을 상기 제1 베이시스 및 상기 제2 베이시스를 이용하여 측정하는 단계;

상기 N개의 통신 주체들 각각이 상기 N-1개의 큐빗 집합들이 인코딩될 때 이용된 베이시스를 각각 예측하여 N-1개의 예측 베이시스를 상기 N-1개의 통신 주체들에 각각 전송하는 단계; 및

상기 N개의 통신 주체들 각각이 상기 N-1개의 통신 주체들로부터 입력 받은 상기 예측 베이시스들이 상기 N-1개의 큐빗 집합들의 인코딩 시에 이용된 인코딩 베이시스들과 일치하는지를 판단하여 상기 예측 베이시스와 상기 인코딩 베이시스의 일치 여부를 상기 N-1개의 통신 주체들에게 전송하는 단계를 포함하고,

상기 N-1 개의 큐빗 집합들 각각은 M개(M은 2 이상의 자연수)의 큐빗들을 포함하는 것을 특징으로 하는 양자 추첨 방법.

청구항 2

제1항에 있어서, 상기 N개의 통신 주체들 각각이 상기 N-1개의 큐빗 집합들을 상기 제1 베이시스 및 상기 제2 베이시스를 이용하여 인코딩하는 단계는

하나의 큐빗 집합 내의 상기 M개의 큐빗들을 모두 동일한 베이시스를 이용하여 인코딩하는 것을 특징으로 하는 양자 추첨 방법.

청구항 3

제2항에 있어서, 상기 N개의 통신 주체들 각각이 상기 N-1개의 통신 주체들에게 상기 N-1개의 큐빗 집합 내의 상기 큐빗들의 상태 시퀀스를 각각 전송하는 단계를 더 포함하는 것을 특징으로 하는 양자 추첨 방법.

청구항 4

제3항에 있어서, 상기 N개의 통신 주체들 각각이 상기 N-1개의 통신 주체들로부터 입력 받은 N-1개의 큐빗 집합들을 상기 제1 베이시스 및 상기 제2 베이시스를 이용하여 측정하는 단계에서,

상기 제1 베이시스를 이용하여 측정하는 큐빗 수는 상기 제2 베이시스를 이용하여 측정하는 큐빗 수와 동일한 것을 특징으로 하는 양자 추첨 방법.

청구항 5

제4항에 있어서, 상기 N개의 통신 주체들 각각이 상기 N-1개의 통신 주체들의 상기 인코딩 베이시스들을 예측하여 맞춘 개수를 기초로 상기 N개의 통신 주체들의 제1 리스트를 생성하는 단계를 더 포함하는 것을 특징으로 하는 양자 추첨 방법.

청구항 6

제5항에 있어서, 상기 N개의 통신 주체들 중 상기 N-1개의 통신 주체들의 상기 인코딩 베이시스들을 예측하여 맞춘 개수가 동일한 제1 그룹의 통신 주체들 간에 양자 추첨을 재수행하여 상기 제1 그룹의 통신 주체들의 우열

을 가리는 단계; 및

상기 제1 리스트 및 상기 제1 그룹의 통신 주체들의 상기 우열을 기초로 제2 리스트를 생성하는 단계를 더 포함하는 것을 특징으로 하는 양자 추첨 방법.

청구항 7

제1항에 있어서, 상기 N개의 통신 주체들은 서로 원거리에 배치되는 것을 특징으로 하는 양자 추첨 방법.

청구항 8

제1항에 있어서, 상기 큐빗은 제1 상태, 제2 상태 및 제3 상태를 갖고,

상기 제1 상태는 $|0\rangle$ 이고, 상기 제2 상태는 $|1\rangle$ 이며,

상기 제3 상태는 $a|0\rangle+b|1\rangle$ 이고, 상기 a^2은 상기 큐빗의 상태가 $|0\rangle$ 일 확률이며, 상기 b^2은 상기 큐빗의 상태가 $|1\rangle$ 일 확률이고,

$|a|^2+|b|^2=1$인 것을 특징으로 하는 양자 추첨 방법.

청구항 9

제8항에 있어서, 상기 큐빗은 광자(Photon)에 의해 전송되는 것을 특징으로 하는 양자 추첨 방법.

청구항 10

제9항에 있어서, 상기 큐빗이 상기 제1 베이시스에 의해 인코딩 및 측정될 때, 상기 큐빗이 수평 방향의 편광을 가지면 상기 큐빗은 상기 제1 상태이고, 상기 큐빗이 수직 방향의 편광을 가지면 상기 큐빗은 상기 제2 상태이며,

상기 큐빗이 상기 제2 베이시스에 의해 인코딩 및 측정될 때, 상기 큐빗이 제1 대각 방향의 편광을 가지면 상기 큐빗은 상기 제1 상태이고, 상기 큐빗이 제2 대각 방향의 편광을 가지면 상기 큐빗은 상기 제2 상태인 것을 특징으로 하는 양자 추첨 방법.

청구항 11

제8항에 있어서, 상기 큐빗은 전자(Electron)에 의해 전송되는 것을 특징으로 하는 양자 추첨 방법.

청구항 12

N개(N은 3 이상의 자연수)의 통신 주체들 각각이 본인을 제외한 다른 N-1개의 통신 주체들에게 각각 전송하기 위한 N-1개의 큐빗 집합들을 생성하는 단계;

상기 N개의 통신 주체들 각각이 상기 N-1개의 큐빗 집합들을 제1 베이시스 및 제2 베이시스를 이용하여 인코딩하는 단계;

상기 N개의 통신 주체들 각각이 인코딩된 상기 N-1개의 큐빗 집합들을 상기 N-1개의 통신 주체들에게 각각 전송하는 단계;

상기 N개의 통신 주체들 각각이 상기 N-1개의 통신 주체들로부터 입력 받은 N-1개의 큐빗 집합들을 상기 제1 베이시스 및 상기 제2 베이시스를 이용하여 측정하는 단계;

상기 N개의 통신 주체들 각각이 상기 N-1개의 큐빗 집합들이 인코딩될 때 이용된 베이시스를 각각 예측하여 N-1개의 예측 베이시스를 상기 N-1개의 통신 주체들에 각각 전송하는 단계;

상기 N개의 통신 주체들 각각이 상기 N-1개의 통신 주체들로부터 입력 받은 상기 예측 베이시스들이 상기 N-1개의 큐빗 집합들의 인코딩 시에 이용된 인코딩 베이시스들과 일치하는지를 판단하여 상기 예측 베이시스와 상기 인코딩 베이시스의 일치 여부를 상기 N-1개의 통신 주체들에게 전송하여 상기 N개의 통신 주체들 사이의 순위를 결정하는 단계; 및

상기 N개의 통신 주체들 사이의 상기 순위를 기초로 자원을 분배하는 단계를 포함하고,

상기 N-1 개의 큐빗 집합들 각각은 M개(M은 2 이상의 자연수)의 큐빗들을 포함하는 것을 특징으로 하는 양자 통신 방법.

청구항 13

제12항에 있어서, 상기 N개의 통신 주체들 각각이 상기 N-1개의 큐빗 집합들을 상기 제1 베이시스 및 상기 제2 베이시스를 이용하여 인코딩하는 단계는

하나의 큐빗 집합 내의 상기 M개의 큐빗들을 모두 동일한 베이시스를 이용하여 인코딩하는 것을 특징으로 하는 양자 통신 방법.

청구항 14

제13항에 있어서, 상기 N개의 통신 주체들 각각이 상기 N-1개의 통신 주체들에게 상기 N-1개의 큐빗 집합 내의 상기 큐빗들의 상태 시퀀스를 각각 전송하는 단계를 더 포함하는 것을 특징으로 하는 양자 통신 방법.

청구항 15

제14항에 있어서, 상기 N개의 통신 주체들 각각이 상기 N-1개의 통신 주체들로부터 입력 받은 N-1개의 큐빗 집합들을 상기 제1 베이시스 및 상기 제2 베이시스를 이용하여 측정하는 단계에서,

상기 제1 베이시스를 이용하여 측정하는 큐빗 수는 상기 제2 베이시스를 이용하여 측정하는 큐빗 수와 동일한 것을 특징으로 하는 양자 통신 방법.

청구항 16

제15항에 있어서, 상기 N개의 통신 주체들 사이의 순위를 결정하는 단계는

상기 N개의 통신 주체들 각각이 상기 N-1개의 통신 주체들의 상기 인코딩 베이시스들을 예측하여 맞춘 개수를 기초로 상기 N개의 통신 주체들의 제1 리스트를 생성하는 단계를 더 포함하는 것을 특징으로 하는 양자 통신 방법.

청구항 17

제16항에 있어서, 상기 N개의 통신 주체들 사이의 순위를 결정하는 단계는

상기 N개의 통신 주체들 중 상기 N-1개의 통신 주체들의 상기 인코딩 베이시스들을 예측하여 맞춘 개수가 동일한 제1 그룹의 통신 주체들 간에 양자 추첨을 재수행하여 상기 제1 그룹의 통신 주체들의 우열을 가리는 단계; 및

상기 제1 리스트 및 상기 제1 그룹의 통신 주체들의 상기 우열을 기초로 제2 리스트를 생성하는 단계를 더 포함하는 것을 특징으로 하는 양자 통신 방법.

청구항 18

서로 통신하는 제1 통신 주체, 제2 통신 주체 및 제3 통신 주체를 포함하고,

상기 제1 통신 주체는 제1 큐빗 집합 및 제2 큐빗 집합을 생성하고, 상기 제1 큐빗 집합 및 상기 제2 큐빗 집합을 제1 베이시스 및 제2 베이시스를 이용하여 인코딩하며, 상기 인코딩된 제1 큐빗 집합을 상기 제2 통신 주체에게 전송하고, 상기 인코딩된 제2 큐빗 집합을 상기 제3 통신 주체에게 전송하며,

상기 제2 통신 주체는 제3 큐빗 집합 및 제4 큐빗 집합을 생성하고, 상기 제3 큐빗 집합 및 상기 제4 큐빗 집합을 상기 제1 베이시스 및 상기 제2 베이시스를 이용하여 인코딩하며, 상기 인코딩된 제3 큐빗 집합을 상기 제1 통신 주체에게 전송하고, 상기 인코딩된 제4 큐빗 집합을 상기 제3 통신 주체에게 전송하며,

상기 제3 통신 주체는 제5 큐빗 집합 및 제6 큐빗 집합을 생성하고, 상기 제5 큐빗 집합 및 상기 제6 큐빗 집합을 상기 제1 베이시스 및 상기 제2 베이시스를 이용하여 인코딩하며, 상기 인코딩된 제5 큐빗 집합을 상기 제1 통신 주체에게 전송하고, 상기 인코딩된 제6 큐빗 집합을 상기 제2 통신 주체에게 전송하며,

상기 제1 통신 주체는 상기 제3 큐빗 집합이 인코딩될 때 이용된 베이시스를 예측하여 상기 제2 통신 주체에게 전송하며, 상기 제5 큐빗 집합이 인코딩될 때 이용된 베이시스를 예측하여 상기 제3 통신 주체에게 전송하며,

상기 제2 통신 주체는 상기 제1 큐빗 집합이 인코딩될 때 이용된 베이시스를 예측하여 상기 제1 통신 주체에게 전송하며, 상기 제6 큐빗 집합이 인코딩될 때 이용된 베이시스를 예측하여 상기 제3 통신 주체에게 전송하며,

상기 제3 통신 주체는 상기 제2 큐빗 집합이 인코딩될 때 이용된 베이시스를 예측하여 상기 제1 통신 주체에게 전송하며, 상기 제4 큐빗 집합이 인코딩될 때 이용된 베이시스를 예측하여 상기 제2 통신 주체에게 전송하고,

상기 제1 내지 제6 큐빗 집합들 각각은 M개(M은 2 이상의 자연수)의 큐빗들을 포함하는 것을 특징으로 하는 양자 통신 시스템.

청구항 19

제18항에 있어서, 상기 제1 통신 주체, 상기 제2 통신 주체 및 상기 제3 통신 주체와 통신하는 제4 통신 주체를 더 포함하고,

상기 제1 통신 주체는 제7 큐빗 집합을 생성 및 인코딩하여, 상기 인코딩된 상기 제7 큐빗 집합을 상기 제4 통신 주체에게 전송하고, 상기 제2 통신 주체는 제8 큐빗 집합을 생성 및 인코딩하여, 상기 인코딩된 상기 제8 큐빗 집합을 상기 제4 통신 주체에게 전송하며, 상기 제3 통신 주체는 제9 큐빗 집합을 생성 및 인코딩하여, 상기 인코딩된 상기 제9 큐빗 집합을 상기 제4 통신 주체에게 전송하고,

상기 제4 통신 주체는 제10 큐빗 집합, 제11 큐빗 집합 및 제12 큐빗 집합을 생성 및 인코딩하여, 상기 제1 통신 주체, 상기 제2 통신 주체 및 상기 제3 통신 주체에게 각각 전송하는 것을 특징으로 하는 양자 통신 시스템.

청구항 20

제19항에 있어서, 상기 제1 통신 주체, 상기 제2 통신 주체, 상기 제3 통신 주체 및 상기 제4 통신 주체와 통신하는 제5 통신 주체를 더 포함하고,

상기 제1 통신 주체는 제13 큐빗 집합을 생성 및 인코딩하여, 상기 인코딩된 상기 제13 큐빗 집합을 상기 제5 통신 주체에게 전송하고, 상기 제2 통신 주체는 제14 큐빗 집합을 생성 및 인코딩하여, 상기 인코딩된 상기 제14 큐빗 집합을 상기 제5 통신 주체에게 전송하며, 상기 제3 통신 주체는 제15 큐빗 집합을 생성 및 인코딩하여, 상기 인코딩된 상기 제15 큐빗 집합을 상기 제5 통신 주체에게 전송하고, 상기 제4 통신 주체는 제16 큐빗 집합을 생성 및 인코딩하여, 상기 인코딩된 상기 제16 큐빗 집합을 상기 제5 통신 주체에게 전송하고,

상기 제5 통신 주체는 제17 큐빗 집합, 제18 큐빗 집합, 제19 큐빗 집합 및 제20 큐빗 집합을 생성 및 인코딩하여, 상기 제1 통신 주체, 상기 제2 통신 주체, 상기 제3 통신 주체 및 상기 제4 통신 주체에게 각각 전송하는 것을 특징으로 하는 양자 통신 시스템.

청구항 21

제18항에 있어서, 상기 제1 내지 제3 통신 주체 각각은

하나의 큐빗 집합 내의 상기 M개의 큐빗들을 모두 동일한 베이시스를 이용하여 인코딩하는 것을 특징으로 하는 양자 통신 시스템.

청구항 22

제21항에 있어서,

상기 제1 통신 주체는 상기 제1 큐빗 집합 내의 상기 큐빗들의 상태 시퀀스를 상기 제2 통신 주체에게 전송하고, 상기 제2 큐빗 집합 내의 상기 큐빗들의 상태 시퀀스를 상기 제3 통신 주체에게 전송하며,

상기 제2 통신 주체는 상기 제3 큐빗 집합 내의 상기 큐빗들의 상태 시퀀스를 상기 제1 통신 주체에게 전송하고, 상기 제4 큐빗 집합 내의 상기 큐빗들의 상태 시퀀스를 상기 제3 통신 주체에게 전송하며,

상기 제3 통신 주체는 상기 제5 큐빗 집합 내의 상기 큐빗들의 상태 시퀀스를 상기 제1 통신 주체에게 전송하고, 상기 제6 큐빗 집합 내의 상기 큐빗들의 상태 시퀀스를 상기 제2 통신 주체에게 전송하는 것을 특징으로 하는 양자 통신 시스템.

청구항 23

제22항에 있어서, 상기 제1 내지 제3 통신 주체 각각이 상기 제1 베이시스를 이용하여 측정하는 큐빗 수는 상기

제2 베이시스를 이용하여 측정하는 큐빗 수와 동일한 것을 특징으로 하는 양자 통신 시스템.

청구항 24

제23항에 있어서, 상기 제1 내지 제3 통신 주체들 각각이 본인을 제외한 상기 제1 내지 제3 통신 주체들의 인코딩 베이시스들을 예측하여 맞춘 개수를 기초로 상기 제1 내지 제3 통신 주체들의 제1 리스트가 생성되는 것을 특징으로 하는 양자 통신 시스템.

청구항 25

제24항에 있어서, 상기 제1 내지 제3 통신 주체들 중 상기 본인을 제외한 상기 제1 내지 제3 통신 주체들의 상기 인코딩 베이시스들을 예측하여 맞춘 개수가 동일한 제1 그룹의 통신 주체들 간에 양자 추첨을 재수행하여 상기 제1 그룹의 통신 주체들의 우열을 가리고,

상기 제1 리스트 및 상기 제1 그룹의 통신 주체들의 상기 우열을 기초로 상기 제1 내지 제3 통신 주체들의 제2 리스트가 생성되는 것을 특징으로 하는 양자 통신 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은 통신 시스템에 관한 것으로, 더욱 상세하게는 양자 통신에서의 양자 추첨 방법, 상기 양자 추첨 방법을 이용하는 양자 통신 방법 및 상기 양자 추첨 방법 및/또는 상기 양자 통신 방법을 수행하는 양자 통신 시스템에 관한 것이다.

배 경 기 술

[0002] 복수의 통신 주체들이 존재하는 통신 시스템에서는 공정한 방식으로 통신 주체들 간의 순위를 정해야 하는 경우가 있다. 상기 통신 시스템 내의 통신 주체들 중 어느 하나가 상기 순위를 정하는 방식을 주관하게 되면 상기 통신 주체들 간의 공정성이 손상될 우려가 있다.

[0003] 그렇지 않으면, 상기 순위를 공정하게 정하기 위해서 별도의 중재 통신 주체가 필요할 수 있다. 그러나 상기 중재 통신 주체가 존재하더라도 상기 중재 통신 주체가 상기 통신 주체들 중 어느 편으로 편향된 결정을 내릴 수 있으므로, 상기 통신 시스템 내의 모든 통신 주체들이 신뢰할 수 있을 만큼 공정하게 순위를 정하는 것은 어려운 문제점이 있다.

발명의 내용

해결하려는 과제

[0004] 본 발명이 이루고자 하는 목적은 양자 통신 방식에 내재되어 있는 공정성을 이용하여 복수의 통신 주체들 간에 공정하게 순위를 정할 수 있는 양자 추첨 방법을 제공하는 것이다.

[0005] 본 발명이 이루고자 하는 다른 목적은 상기 양자 추첨 방법을 이용하는 양자 통신 방법을 제공하는 것이다.

[0006] 본 발명이 이루고자 하는 또 다른 목적은 상기 양자 추첨 방법 및 상기 양자 통신 방법을 수행하는 양자 통신 시스템을 제공하는 것이다.

과제의 해결 수단

[0007] 상기한 본 발명의 목적을 실현하기 위한 일 실시예에 따른 양자 추첨 방법은 N개(N은 3 이상의 자연수)의 통신 주체들 각각이 본인을 제외한 다른 N-1개의 통신 주체들에게 각각 전송하기 위한 N-1개의 큐빗 집합들을 생성하는 단계, 상기 N개의 통신 주체들 각각이 상기 N-1개의 큐빗 집합들을 제1 베이시스 및 제2 베이시스를 이용하여 인코딩하는 단계, 상기 N개의 통신 주체들 각각이 인코딩된 상기 N-1개의 큐빗 집합들을 상기 N-1개의 통신 주체들에게 각각 전송하는 단계, 상기 N개의 통신 주체들 각각이 상기 N-1개의 통신 주체들로부터 입력 받은 N-1개의 큐빗 집합들을 상기 제1 베이시스 및 상기 제2 베이시스를 이용하여 측정하는 단계, 상기 N개의 통신 주체들 각각이 상기 N-1개의 큐빗 집합들이 인코딩될 때 이용된 베이시스를 각각 예측하여 N-1개의 예측 베이시스를 상기 N-1개의 통신 주체들에 각각 전송하는 단계 및 상기 N개의 통신 주체들 각각이 상기 N-1개의 통신 주체

들로부터 입력 받은 상기 예측 베이시스들이 상기 N-1개의 큐빗 집합들의 인코딩 시에 이용된 인코딩 베이시스들과 일치하는지를 판단하여 상기 예측 베이시스와 상기 인코딩 베이시스의 일치 여부를 상기 N-1개의 통신 주체들에게 전송하는 단계를 포함한다. 상기 N-1 개의 큐빗 집합들 각각은 M개(M은 2 이상의 자연수)의 큐빗들을 포함한다.

[0008] 본 발명의 일 실시예에 있어서, 상기 N개의 통신 주체들 각각이 상기 N-1개의 큐빗 집합들을 상기 제1 베이시스 및 상기 제2 베이시스를 이용하여 인코딩하는 단계는 하나의 큐빗 집합 내의 상기 M개의 큐빗들을 모두 동일한 베이시스를 이용하여 인코딩할 수 있다.

[0009] 본 발명의 일 실시예에 있어서, 상기 양자 추첨 방법은 상기 N개의 통신 주체들 각각이 상기 N-1개의 통신 주체들에게 상기 N-1개의 큐빗 집합 내의 상기 큐빗들의 상태 시퀀스를 각각 전송하는 단계를 더 포함할 수 있다.

[0010] 본 발명의 일 실시예에 있어서, 상기 N개의 통신 주체들 각각이 상기 N-1개의 통신 주체들로부터 입력 받은 N-1개의 큐빗 집합들을 상기 제1 베이시스 및 상기 제2 베이시스를 이용하여 측정하는 단계에서, 상기 제1 베이시스를 이용하여 측정하는 큐빗 수는 상기 제2 베이시스를 이용하여 측정하는 큐빗 수와 동일할 수 있다.

[0011] 본 발명의 일 실시예에 있어서, 상기 양자 추첨 방법은 상기 N개의 통신 주체들 각각이 상기 N-1개의 통신 주체들의 상기 인코딩 베이시스들을 예측하여 맞춘 개수를 기초로 상기 N개의 통신 주체들의 제1 리스트를 생성하는 단계를 더 포함할 수 있다.

[0012] 본 발명의 일 실시예에 있어서, 상기 양자 추첨 방법은 상기 N개의 통신 주체들 중 상기 N-1개의 통신 주체들의 상기 인코딩 베이시스들을 예측하여 맞춘 개수가 동일한 제1 그룹의 통신 주체들 간에 양자 추첨을 재수행하여 상기 제1 그룹의 통신 주체들의 우열을 가리는 단계 및 상기 제1 리스트 및 상기 제1 그룹의 통신 주체들의 상기 우열을 기초로 제2 리스트를 생성하는 단계를 더 포함할 수 있다.

[0013] 본 발명의 일 실시예에 있어서, 상기 N개의 통신 주체들은 서로 원거리에 배치될 수 있다.

[0014] 본 발명의 일 실시예에 있어서, 상기 큐빗은 제1 상태, 제2 상태 및 제3 상태를 가질 수 있다. 상기 제1 상태는 |0〉이고, 상기 제2 상태는 |1〉일 수 있다. 상기 제3 상태는 a|0〉+b|1〉이고, 상기 a^2은 상기 큐빗의 상태가 |0〉일 확률이며, 상기 b^2은 상기 큐빗의 상태가 |1〉일 확률일 수 있다. $|a|^2+|b|^2=1$일 수 있다.

[0015] 본 발명의 일 실시예에 있어서, 상기 큐빗은 광자(Photon)에 의해 전송될 수 있다.

[0016] 본 발명의 일 실시예에 있어서, 상기 큐빗이 상기 제1 베이시스에 의해 인코딩 및 측정될 때, 상기 큐빗이 수평 방향의 편광을 가지면 상기 큐빗은 상기 제1 상태이고, 상기 큐빗이 수직 방향의 편광을 가지면 상기 큐빗은 상기 제2 상태일 수 있다. 상기 큐빗이 상기 제2 베이시스에 의해 인코딩 및 측정될 때, 상기 큐빗이 제1 대각 방향의 편광을 가지면 상기 큐빗은 상기 제1 상태이고, 상기 큐빗이 제2 대각 방향의 편광을 가지면 상기 큐빗은 상기 제2 상태일 수 있다.

[0017] 본 발명의 일 실시예에 있어서, 상기 큐빗은 전자(Electron)에 의해 전송될 수 있다.

[0018] 상기한 본 발명의 목적을 실현하기 위한 일 실시예에 따른 양자 통신 방법은 N개(N은 3 이상의 자연수)의 통신 주체들 각각이 본인을 제외한 다른 N-1개의 통신 주체들에게 각각 전송하기 위한 N-1개의 큐빗 집합들을 생성하는 단계, 상기 N개의 통신 주체들 각각이 상기 N-1개의 큐빗 집합들을 제1 베이시스 및 제2 베이시스를 이용하여 인코딩하는 단계, 상기 N개의 통신 주체들 각각이 인코딩된 상기 N-1개의 큐빗 집합들을 상기 N-1개의 통신 주체들에게 각각 전송하는 단계, 상기 N개의 통신 주체들 각각이 상기 N-1개의 통신 주체들로부터 입력 받은 N-1개의 큐빗 집합들을 상기 제1 베이시스 및 상기 제2 베이시스를 이용하여 측정하는 단계, 상기 N개의 통신 주체들 각각이 상기 N-1개의 큐빗 집합들이 인코딩될 때 이용된 베이시스를 각각 예측하여 N-1개의 예측 베이시스를 상기 N-1개의 통신 주체들에 각각 전송하는 단계, 상기 N개의 통신 주체들 각각이 상기 N-1개의 통신 주체들로부터 입력 받은 상기 예측 베이시스들이 상기 N-1개의 큐빗 집합들의 인코딩 시에 이용된 인코딩 베이시스들과 일치하는지를 판단하여 상기 예측 베이시스와 상기 인코딩 베이시스의 일치 여부를 상기 N-1개의 통신 주체들에게 전송하여 상기 N개의 통신 주체들 사이의 순위를 결정하는 단계 및 상기 N개의 통신 주체들 사이의 상기 순위를 기초로 자원을 분배하는 단계를 포함한다. 상기 N-1 개의 큐빗 집합들 각각은 M개(M은 2 이상의 자연수)의 큐빗들을 포함한다.

[0019] 본 발명의 일 실시예에 있어서, 상기 N개의 통신 주체들 각각이 상기 N-1개의 큐빗 집합들을 상기 제1 베이시스 및 상기 제2 베이시스를 이용하여 인코딩하는 단계는 하나의 큐빗 집합 내의 상기 M개의 큐빗들을 모두 동일한

베이시스를 이용하여 인코딩할 수 있다.

[0020] 본 발명의 일 실시예에 있어서, 상기 양자 통신 방법은 상기 N개의 통신 주체들 각각이 상기 N-1개의 통신 주체들에게 상기 N-1개의 큐빗 집합 내의 상기 큐빗들의 상태 시퀀스를 각각 전송하는 단계를 더 포함할 수 있다.

[0021] 본 발명의 일 실시예에 있어서, 상기 N개의 통신 주체들 각각이 상기 N-1개의 통신 주체들로부터 입력 받은 N-1개의 큐빗 집합들을 상기 제1 베이시스 및 상기 제2 베이시스를 이용하여 측정하는 단계에서, 상기 제1 베이시스를 이용하여 측정하는 큐빗 수는 상기 제2 베이시스를 이용하여 측정하는 큐빗 수와 동일할 수 있다.

[0022] 본 발명의 일 실시예에 있어서, 상기 N개의 통신 주체들 사이의 순위를 결정하는 단계는 상기 N개의 통신 주체들 각각이 상기 N-1개의 통신 주체들의 상기 인코딩 베이시스들을 예측하여 맞춘 개수를 기초로 상기 N개의 통신 주체들의 제1 리스트를 생성하는 단계를 더 포함할 수 있다.

[0023] 본 발명의 일 실시예에 있어서, 상기 N개의 통신 주체들 사이의 순위를 결정하는 단계는 상기 N개의 통신 주체들 중 상기 N-1개의 통신 주체들의 상기 인코딩 베이시스들을 예측하여 맞춘 개수가 동일한 제1 그룹의 통신 주체들 간에 양자 추첨을 재수행하여 상기 제1 그룹의 통신 주체들의 우열을 가리는 단계 및 상기 제1 리스트 및 상기 제1 그룹의 통신 주체들의 상기 우열을 기초로 제2 리스트를 생성하는 단계를 더 포함할 수 있다.

[0024] 상기한 본 발명의 목적을 실현하기 위한 일 실시예에 따른 양자 통신 시스템은 서로 통신하는 제1 통신 주체, 제2 통신 주체 및 제3 통신 주체를 포함한다. 상기 제1 통신 주체는 제1 큐빗 집합 및 제2 큐빗 집합을 생성하고, 상기 제1 큐빗 집합 및 상기 제2 큐빗 집합을 제1 베이시스 및 제2 베이시스를 이용하여 인코딩하며, 상기 인코딩된 제1 큐빗 집합을 상기 제2 통신 주체에게 전송하고, 상기 인코딩된 제2 큐빗 집합을 상기 제3 통신 주체에게 전송한다. 상기 제2 통신 주체는 제3 큐빗 집합 및 제4 큐빗 집합을 생성하고, 상기 제3 큐빗 집합 및 상기 제4 큐빗 집합을 상기 제1 베이시스 및 상기 제2 베이시스를 이용하여 인코딩하며, 상기 인코딩된 제3 큐빗 집합을 상기 제1 통신 주체에게 전송하고, 상기 인코딩된 제4 큐빗 집합을 상기 제3 통신 주체에게 전송한다. 상기 제3 통신 주체는 제5 큐빗 집합 및 제6 큐빗 집합을 생성하고, 상기 제5 큐빗 집합 및 상기 제6 큐빗 집합을 상기 제1 베이시스 및 상기 제2 베이시스를 이용하여 인코딩하며, 상기 인코딩된 제5 큐빗 집합을 상기 제1 통신 주체에게 전송하고, 상기 인코딩된 제6 큐빗 집합을 상기 제2 통신 주체에게 전송한다. 상기 제1 통신 주체는 상기 제3 큐빗 집합이 인코딩될 때 이용된 베이시스를 예측하여 상기 제2 통신 주체에게 전송하며, 상기 제5 큐빗 집합이 인코딩될 때 이용된 베이시스를 예측하여 상기 제3 통신 주체에게 전송한다. 상기 제2 통신 주체는 상기 제1 큐빗 집합이 인코딩될 때 이용된 베이시스를 예측하여 상기 제1 통신 주체에게 전송하며, 상기 제6 큐빗 집합이 인코딩될 때 이용된 베이시스를 예측하여 상기 제3 통신 주체에게 전송한다. 상기 제3 통신 주체는 상기 제2 큐빗 집합이 인코딩될 때 이용된 베이시스를 예측하여 상기 제1 통신 주체에게 전송하며, 상기 제4 큐빗 집합이 인코딩될 때 이용된 베이시스를 예측하여 상기 제2 통신 주체에게 전송한다. 상기 제1 내지 제6 큐빗 집합들 각각은 M개(M은 2 이상의 자연수)의 큐빗들을 포함한다.

[0025] 본 발명의 일 실시예에 있어서, 상기 양자 통신 시스템은 상기 제1 통신 주체, 상기 제2 통신 주체 및 상기 제3 통신 주체와 통신하는 제4 통신 주체를 더 포함할 수 있다. 상기 제1 통신 주체는 제7 큐빗 집합을 생성 및 인코딩하여, 상기 인코딩된 상기 제7 큐빗 집합을 상기 제4 통신 주체에게 전송하고, 상기 제2 통신 주체는 제8 큐빗 집합을 생성 및 인코딩하여, 상기 인코딩된 상기 제8 큐빗 집합을 상기 제4 통신 주체에게 전송하며, 상기 제3 통신 주체는 제9 큐빗 집합을 생성 및 인코딩하여, 상기 인코딩된 상기 제9 큐빗 집합을 상기 제4 통신 주체에게 전송할 수 있다. 상기 제4 통신 주체는 제10 큐빗 집합, 제11 큐빗 집합 및 제12 큐빗 집합을 생성 및 인코딩하여, 상기 제1 통신 주체, 상기 제2 통신 주체 및 상기 제3 통신 주체에게 각각 전송할 수 있다.

[0026] 본 발명의 일 실시예에 있어서, 상기 양자 통신 시스템은 상기 제1 통신 주체, 상기 제2 통신 주체, 상기 제3 통신 주체 및 상기 제4 통신 주체와 통신하는 제5 통신 주체를 더 포함할 수 있다. 상기 제1 통신 주체는 제13 큐빗 집합을 생성 및 인코딩하여, 상기 인코딩된 상기 제13 큐빗 집합을 상기 제5 통신 주체에게 전송하고, 상기 제2 통신 주체는 제14 큐빗 집합을 생성 및 인코딩하여, 상기 인코딩된 상기 제14 큐빗 집합을 상기 제5 통신 주체에게 전송하며, 상기 제3 통신 주체는 제15 큐빗 집합을 생성 및 인코딩하여, 상기 인코딩된 상기 제15 큐빗 집합을 상기 제5 통신 주체에게 전송하고, 상기 제4 통신 주체는 제16 큐빗 집합을 생성 및 인코딩하여, 상기 인코딩된 상기 제16 큐빗 집합을 상기 제5 통신 주체에게 전송할 수 있다. 상기 제5 통신 주체는 제17 큐빗 집합, 제18 큐빗 집합, 제19 큐빗 집합 및 제20 큐빗 집합을 생성 및 인코딩하여, 상기 제1 통신 주체, 상기 제2 통신 주체, 상기 제3 통신 주체 및 상기 제4 통신 주체에게 각각 전송할 수 있다.

[0027] 본 발명의 일 실시예에 있어서, 상기 제1 내지 제3 통신 주체 각각은 하나의 큐빗 집합 내의 상기 M개의 큐빗들

을 모두 동일한 베이시스를 이용하여 인코딩할 수 있다.

[0028] 본 발명의 일 실시예에 있어서, 상기 제1 통신 주체는 상기 제1 큐빗 집합 내의 상기 큐빗들의 상태 시퀀스를 상기 제2 통신 주체에게 전송하고, 상기 제2 큐빗 집합 내의 상기 큐빗들의 상태 시퀀스를 상기 제3 통신 주체에게 전송할 수 있다. 상기 제2 통신 주체는 상기 제3 큐빗 집합 내의 상기 큐빗들의 상태 시퀀스를 상기 제1 통신 주체에게 전송하고, 상기 제4 큐빗 집합 내의 상기 큐빗들의 상태 시퀀스를 상기 제3 통신 주체에게 전송할 수 있다. 상기 제3 통신 주체는 상기 제5 큐빗 집합 내의 상기 큐빗들의 상태 시퀀스를 상기 제1 통신 주체에게 전송하고, 상기 제6 큐빗 집합 내의 상기 큐빗들의 상태 시퀀스를 상기 제2 통신 주체에게 전송할 수 있다.

[0029] 본 발명의 일 실시예에 있어서, 상기 제1 내지 제3 통신 주체 각각이 상기 제1 베이시스를 이용하여 측정하는 큐빗 수는 상기 제2 베이시스를 이용하여 측정하는 큐빗 수와 동일할 수 있다.

[0030] 본 발명의 일 실시예에 있어서, 상기 제1 내지 제3 통신 주체들 각각이 본인을 제외한 상기 제1 내지 제3 통신 주체들의 인코딩 베이시스들을 예측하여 맞춘 개수를 기초로 상기 제1 내지 제3 통신 주체들의 제1 리스트가 생성될 수 있다.

[0031] 본 발명의 일 실시예에 있어서, 상기 제1 내지 제3 통신 주체들 중 상기 본인을 제외한 상기 제1 내지 제3 통신 주체들의 상기 인코딩 베이시스들을 예측하여 맞춘 개수가 동일한 제1 그룹의 통신 주체들 간에 양자 추첨을 재수행하여 상기 제1 그룹의 통신 주체들의 우열을 가릴 수 있다. 상기 제1 리스트 및 상기 제1 그룹의 통신 주체들의 상기 우열을 기초로 상기 제1 내지 제3 통신 주체들의 제2 리스트가 생성될 수 있다.

발명의 효과

[0032] 상기와 같은 본 발명의 실시예들에 따른 양자 추첨 방법, 이를 이용한 양자 통신 방법 및 이를 수행하는 양자 통신 시스템에서는, 양자 통신 방식에 내재되어 있는 공정성을 이용하여 별도의 중재 통신 주체 없이도 복수의 통신 주체들 간에 공정하게 순위를 정할 수 있다.

[0033] 또한, 상기 정해진 상기 통신 주체들 간의 공정한 순위를 기초로 상기 통신 주체들 간에 공정하게 자원을 분배할 수 있다.

도면의 간단한 설명

[0034] 도 1은 본 발명의 일 실시예에 따른 양자 통신 시스템을 나타내는 개념도이다.

도 2a는 도 1의 양자 통신 시스템에서 큐빗의 제1 베이시스를 나타내는 개념도이다.

도 2b는 도 1의 양자 통신 시스템에서 상기 큐빗의 제2 베이시스를 나타내는 개념도이다.

도 3은 도 1의 양자 통신 시스템에서 상기 큐빗의 제1 베이시스 및 제2 베이시스에 따른 제1 상태 및 제2 상태를 나타내는 표이다.

도 4는 도 1의 양자 통신 시스템에서 제1 통신 주체 및 제2 통신 주체의 동작의 일례를 나타내는 표이다.

도 5는 도 1의 양자 통신 시스템에서 제1 통신 주체 및 제4 통신 주체의 동작의 일례를 나타내는 표이다.

도 6a는 도 1의 양자 통신 시스템에서 제1 통신 주체가 다른 통신 주체들에게 통지하는 정보의 일례를 나타내는 표이다.

도 6b는 도 1의 양자 통신 시스템에서 제2 통신 주체가 다른 통신 주체들에게 통지하는 정보의 일례를 나타내는 표이다.

도 6c는 도 1의 양자 통신 시스템에서 제3 통신 주체가 다른 통신 주체들에게 통지하는 정보의 일례를 나타내는 표이다.

도 6d는 도 1의 양자 통신 시스템에서 제4 통신 주체가 다른 통신 주체들에게 통지하는 정보의 일례를 나타내는 표이다.

도 6e는 도 1의 양자 통신 시스템에서 제5 통신 주체가 다른 통신 주체들에게 통지하는 정보의 일례를 나타내는 표이다.

도 7은 도 1의 양자 통신 시스템에서 예측 베이시스와 인코딩 베이시스의 일치 여부의 개수를 기초로 생성되는

제1 리스트이다.

도 8은 도 1의 양자 통신 시스템에서 예측 베이시스와 인코딩 베이시스의 일치 여부의 개수를 기초로 생성되는 제2 리스트이다.

발명을 실시하기 위한 구체적인 내용

[0035] 본문에 개시되어 있는 본 발명의 실시예들에 대해서, 특정한 구조적 내지 기능적 설명들은 단지 본 발명의 실시예를 설명하기 위한 목적으로 예시된 것으로, 본 발명의 실시예들은 다양한 형태로 실시될 수 있으며 본문에 설명된 실시예들에 한정되는 것으로 해석되어서는 아니 된다.

[0036] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 형태를 가질 수 있는바, 특정 실시예들을 도면에 예시하고 본문에 상세하게 설명하고자 한다. 그러나 이는 본 발명을 특정한 개시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다.

[0037] 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 목적으로 사용될 수 있다. 예를 들어, 본 발명의 권리 범위로부터 이탈되지 않은 채 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다.

[0038] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다. 구성요소들 간의 관계를 설명하는 다른 표현들, 즉 "~사이에"와 "바로 ~사이에" 또는 "~에 이웃하는"과 "~에 직접 이웃하는" 등도 마찬가지로 해석되어야 한다.

[0039] 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 설시된 특징, 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0040] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미이다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미인 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0041] 한편, 어떤 실시예가 달리 구현 가능한 경우에 특정 블록 내에 명기된 기능 또는 동작이 순서도에 명기된 순서와 다르게 일어날 수도 있다. 예를 들어, 연속하는 두 블록이 실제로는 실질적으로 동시에 수행될 수도 있고, 관련된 기능 또는 동작에 따라서는 상기 블록들이 거꾸로 수행될 수도 있다.

[0042] 이하, 첨부한 도면들을 참조하여, 본 발명의 바람직한 실시예를 보다 상세하게 설명하고자 한다. 도면상의 동일한 구성요소에 대해서는 동일한 참조부호를 사용하고 동일한 구성요소에 대해서 중복된 설명은 생략한다.

[0043] 도 1은 본 발명의 일 실시예에 따른 양자 통신 시스템을 나타내는 개념도이다.

[0044] 도 1을 참조하면, 상기 양자 통신 시스템은 N개의 통신 주체들을 포함한다. N은 3이상의 자연수일 수 있다. 도 1에서 상기 양자 통신 시스템 내에는 5개의 통신 주체들(P1 내지 P5)이 존재하는 것으로 예시하였다.

[0045] 본 실시예의 양자 추첨 방법을 수행하기 위해 N개의 통신 주체들 각각은 본인을 제외한 다른 N-1개의 통신 주체들에게 각각 전송하기 위한 N-1개의 큐빗 집합들을 생성한다.

[0046] 예를 들어, 제1 통신 주체(P1)는 제2 내지 제5 통신 주체들(P2 내지 P5)에게 전송하기 위한 4개의 큐빗 집합들을 생성한다. 상기 4개의 큐빗 집합들 각각은 M개의 큐빗들을 포함한다. M은 2 이상의 자연수일 수 있다. M은 10 이상의 자연수일 수 있다. M이 크면 상기 양자 추첨이 안정적으로 수행될 수 있으나 M이 커짐에 따라 통신 데이터 양이 많아지는 문제가 있을 수 있다. 예를 들어, 상기 M은 20일 수 있다. 도 4 및 도 5에서는 M이 15인

경우를 예시하였다.

[0047] 예를 들어, 제2 통신 주체(P2)는 제1, 제3 내지 제5 통신 주체들(P1, P3, P4, P5)에게 전송하기 위한 4개의 큐빗 집합들을 생성한다. 예를 들어, 제3 통신 주체(P3)는 제1, 제2, 제4 및 제5 통신 주체들(P1, P2, P4, P5)에게 전송하기 위한 4개의 큐빗 집합들을 생성한다. 예를 들어, 제4 통신 주체(P4)는 제1 내지 제3 및 제5 통신 주체들(P1, P2, P3, P5)에게 전송하기 위한 4개의 큐빗 집합들을 생성한다. 예를 들어, 제5 통신 주체(P5)는 제1 내지 제4 통신 주체들(P1 내지 P4)에게 전송하기 위한 4개의 큐빗 집합들을 생성한다.

[0048] 상기 N개의 통신 주체들 각각은 상기 생성된 N-1개의 큐빗 집합들을 제1 베이시스 및 제2 베이시스를 이용하여 인코딩한다. 예를 들어, 상기 제1 통신 주체(P1)는 상기 제2 내지 제5 통신 주체들(P2 내지 P5)에게 전송하기 위한 4개의 큐빗 집합들을 제1 베이시스 및 제2 베이시스를 이용하여 각각 인코딩한다.

[0049] 상기 N개의 통신 주체들 각각이 상기 N-1개의 큐빗 집합들을 상기 제1 베이시스 및 상기 제2 베이시스를 이용하여 인코딩할 때, 하나의 큐빗 집합 내의 상기 M개의 큐빗들을 모두 동일한 베이시스를 이용하여 인코딩할 수 있다. 예를 들어, 상기 제1 통신 주체(P1)는 상기 제2 통신 주체(P2)에게 전송하는 제1 큐빗 집합 내의 M개의 큐빗들을 상기 제1 베이시스 또는 상기 제2 베이시스 중 하나를 이용하여 인코딩한다. 상기 제1 큐빗 집합 내의 M개의 큐빗들은 모두 동일한 베이시스를 이용하여 인코딩된다.

[0050] 예를 들어, 상기 제1 통신 주체(P1)는 상기 제2 통신 주체(P2)에게 전송하는 제1 큐빗 집합 내의 M개의 큐빗들을 모두 제1 베이시스를 이용하여 인코딩할 수 있다. 예를 들어, 상기 제1 통신 주체(P1)는 상기 제3 통신 주체(P3)에게 전송하는 제2 큐빗 집합 내의 M개의 큐빗들을 모두 제2 베이시스를 이용하여 인코딩할 수 있다. 예를 들어, 상기 제1 통신 주체(P1)는 상기 제4 통신 주체(P4)에게 전송하는 제3 큐빗 집합 내의 M개의 큐빗들을 모두 제2 베이시스를 이용하여 인코딩할 수 있다. 예를 들어, 상기 제1 통신 주체(P1)는 상기 제5 통신 주체(P5)에게 전송하는 제4 큐빗 집합 내의 M개의 큐빗들을 모두 제1 베이시스를 이용하여 인코딩할 수 있다.

[0051] 모두 설명하지 않았으나, 상기 제2 통신 주체(P2) 내지 상기 제5 통신 주체(P5)도 상기 제1 통신 주체(P1)와 같은 방식으로 상기 큐빗 집합들을 인코딩할 수 있다.

[0052] 예를 들어, 상기 큐빗은 광자(Photon)에 의해 전송될 수 있다. 이와는 달리, 상기 큐빗은 전자(Electron)에 의해 전송될 수 있다.

[0053] 상기 큐빗이 광자(Photon)에 의해 전송될 때, 상기 제1 베이시스는 수직 수평 베이시스(RECTILINEAR BASIS)일 수 있고, 상기 제2 베이시스는 대각 베이시스(DIAGONAL BASIS)일 수 있다. 상기 큐빗의 상태 및 베이시스에 대해서는 도 2a, 도 2b 및 도 3을 참조하여 상세히 설명한다.

[0054] 상기 N개의 통신 주체들 각각은 인코딩된 상기 N-1개의 큐빗 집합들을 상기 N-1개의 통신 주체들에게 각각 전송한다.

[0055] 예를 들어, 상기 제1 통신 주체(P1)는 상기 인코딩된 제1 큐빗 집합을 상기 제2 통신 주체(P2)에게 전송한다. 예를 들어, 상기 제1 통신 주체(P1)는 상기 인코딩된 제2 큐빗 집합을 상기 제3 통신 주체(P3)에게 전송한다. 예를 들어, 상기 제1 통신 주체(P1)는 상기 인코딩된 제3 큐빗 집합을 상기 제4 통신 주체(P4)에게 전송한다. 예를 들어, 상기 제1 통신 주체(P1)는 상기 인코딩된 제4 큐빗 집합을 상기 제5 통신 주체(P5)에게 전송한다.

[0056] 모두 설명하지 않았으나, 상기 제2 통신 주체(P2) 내지 상기 제5 통신 주체(P5)도 상기 제1 통신 주체(P1)와 같은 방식으로 상기 큐빗 집합들을 다른 통신 주체들에게 전송할 수 있다.

[0057] 상기 N개의 통신 주체들 각각은 상기 N-1개의 통신 주체들로부터 입력 받은 N-1개의 큐빗 집합들을 상기 제1 베이시스 및 상기 제2 베이시스를 이용하여 측정한다.

[0058] 예를 들어, 상기 제1 통신 주체(P1)는 상기 제2 통신 주체(P2)로부터 입력 받은 큐빗 집합을 상기 제1 베이시스 및 상기 제2 베이시스를 이용하여 측정한다. 이 때, 상기 제1 통신 주체(P1)는 상기 큐빗 집합을 각 큐빗 단위로 다른 베이시스를 이용하여 측정할 수 있다. 예를 들어, 상기 제1 통신 주체(P1)는 상기 제2 통신 주체(P2)로부터 입력 받은 큐빗 집합 내의 첫 번째 큐빗은 상기 제1 베이시스를 이용하여 상기 큐빗 집합 내의 두 번째 큐빗은 상기 제2 베이시스를 이용하여 측정할 수 있다. 또한, 상기 제1 통신 주체(P1)는 상기 제2 통신 주체(P2)로부터 입력 받은 큐빗 집합 내의 큐빗 중 일부는 측정하지 않고 스킵할 수 있다. 예를 들어, 상기 제1 통신 주체(P1)는 상기 제2 통신 주체(P2)로부터 입력 받은 큐빗 집합 내의 첫 번째 큐빗은 상기 제1 베이시스를 이용하여 상기 큐빗 집합 내의 두 번째 큐빗은 상기 제2 베이시스를 이용하여 측정하며, 상기 큐빗 집합 내의 세 번째

큐빗은 측정하지 않고 스킵할 수 있다.

[0059] 예를 들어, 상기 하나의 큐빗 집합 내에서 상기 제1 베이시스를 이용하여 측정하는 큐빗 수는 상기 제2 베이시스를 이용하여 측정하는 큐빗 수와 동일할 수 있다.

[0060] 예를 들어, 상기 제1 통신 주체(P1)는 상기 제3 통신 주체(P3)로부터 입력 받은 큐빗 집합을 상기 제1 베이시스 및 상기 제2 베이시스를 이용하여 측정한다. 예를 들어, 상기 제1 통신 주체(P1)는 상기 제4 통신 주체(P4)로부터 입력 받은 큐빗 집합을 상기 제1 베이시스 및 상기 제2 베이시스를 이용하여 측정한다. 예를 들어, 상기 제1 통신 주체(P1)는 상기 제5 통신 주체(P5)로부터 입력 받은 큐빗 집합을 상기 제1 베이시스 및 상기 제2 베이시스를 이용하여 측정한다.

[0061] 모두 설명하지 않았으나, 상기 제2 통신 주체(P2) 내지 상기 제5 통신 주체(P5)도 상기 제1 통신 주체(P1)와 같은 방식으로 상기 큐빗 집합들을 측정할 수 있다.

[0062] 상기 N개의 통신 주체들 각각은 상기 N-1개의 큐빗 집합들이 인코딩될 때 이용된 베이시스를 각각 예측하여 N-1개의 예측 베이시스를 상기 N-1개의 통신 주체들에 각각 전송한다.

[0063] 예를 들어, 상기 제1 통신 주체(P1)는 상기 제2 통신 주체(P2)로부터 받은 큐빗 집합이 인코딩될 때 이용된 베이시스를 예측하여 상기 제2 통신 주체(P2)에게 제1 예측 베이시스를 전송한다. 예를 들어, 상기 제1 통신 주체(P1)는 상기 제3 통신 주체(P3)로부터 받은 큐빗 집합이 인코딩될 때 이용된 베이시스를 예측하여 상기 제3 통신 주체(P3)에게 제2 예측 베이시스를 전송한다. 예를 들어, 상기 제1 통신 주체(P1)는 상기 제4 통신 주체(P4)로부터 받은 큐빗 집합이 인코딩될 때 이용된 베이시스를 예측하여 상기 제4 통신 주체(P4)에게 제4 예측 베이시스를 전송한다. 예를 들어, 상기 제1 통신 주체(P1)는 상기 제5 통신 주체(P5)로부터 받은 큐빗 집합이 인코딩될 때 이용된 베이시스를 예측하여 상기 제5 통신 주체(P5)에게 제4 예측 베이시스를 전송한다.

[0064] 모두 설명하지 않았으나, 상기 제2 통신 주체(P2) 내지 상기 제5 통신 주체(P5)도 상기 제1 통신 주체(P1)와 같은 방식으로 상기 예측 베이시스를 다른 통신 주체들에게 전송할 수 있다.

[0065] 상기 N개의 통신 주체들 각각이 상기 N-1개의 통신 주체들로부터 입력 받은 상기 예측 베이시스들이 상기 N-1개의 큐빗 집합들의 인코딩 시에 이용된 인코딩 베이시스들과 일치하는지를 판단하여 상기 예측 베이시스와 상기 인코딩 베이시스의 일치 여부를 상기 N-1개의 통신 주체들에게 전송한다.

[0066] 예를 들어, 상기 제1 통신 주체(P1)가 상기 제2 통신 주체(P2)로부터 받은 큐빗 집합이 인코딩될 때 이용된 베이시스를 예측하여 상기 제2 통신 주체(P2)에게 상기 제1 예측 베이시스를 전송하면, 상기 제2 통신 주체(P2)는 상기 제2 통신 주체(P2)가 상기 제1 통신 주체(P1)에게 전송한 상기 큐빗 집합의 인코딩 시에 이용된 인코딩 베이시스가 상기 제1 통신 주체(P1)로부터 수신한 상기 제1 예측 베이시스와 일치하는지 판단한다. 상기 제2 통신 주체(P2)가 상기 제1 통신 주체(P1)에게 전송한 상기 큐빗 집합의 인코딩 시에 이용된 인코딩 베이시스가 상기 제1 통신 주체(P1)로부터 수신한 상기 제1 예측 베이시스와 일치하면, 상기 제1 통신 주체(P1)는 상기 제2 통신 주체(P2)의 인코딩 베이시스를 맞춘 것이 된다(RIGHT). 상기 제2 통신 주체(P2)가 상기 제1 통신 주체(P1)에게 전송한 상기 큐빗 집합의 인코딩 시에 이용된 인코딩 베이시스가 상기 제1 통신 주체(P1)로부터 수신한 상기 제1 예측 베이시스와 일치하지 않으면, 상기 제1 통신 주체(P1)는 상기 제2 통신 주체(P2)의 인코딩 베이시스를 맞추지 못한 것이 된다(WRONG).

[0067] 예를 들어, 상기 제1 통신 주체(P1)가 상기 제3 통신 주체(P3)로부터 받은 큐빗 집합이 인코딩될 때 이용된 베이시스를 예측하여 상기 제3 통신 주체(P3)에게 상기 제2 예측 베이시스를 전송하면, 상기 제3 통신 주체(P3)는 상기 제3 통신 주체(P3)가 상기 제1 통신 주체(P1)에게 전송한 상기 큐빗 집합의 인코딩 시에 이용된 인코딩 베이시스가 상기 제1 통신 주체(P1)로부터 수신한 상기 제2 예측 베이시스와 일치하는지 판단한다.

[0068] 예를 들어, 상기 제1 통신 주체(P1)가 상기 제4 통신 주체(P4)로부터 받은 큐빗 집합이 인코딩될 때 이용된 베이시스를 예측하여 상기 제4 통신 주체(P4)에게 상기 제3 예측 베이시스를 전송하면, 상기 제4 통신 주체(P4)는 상기 제4 통신 주체(P4)가 상기 제1 통신 주체(P1)에게 전송한 상기 큐빗 집합의 인코딩 시에 이용된 인코딩 베이시스가 상기 제1 통신 주체(P1)로부터 수신한 상기 제3 예측 베이시스와 일치하는지 판단한다.

[0069] 예를 들어, 상기 제1 통신 주체(P1)가 상기 제5 통신 주체(P5)로부터 받은 큐빗 집합이 인코딩될 때 이용된 베이시스를 예측하여 상기 제5 통신 주체(P5)에게 상기 제4 예측 베이시스를 전송하면, 상기 제5 통신 주체(P5)는 상기 제5 통신 주체(P5)가 상기 제1 통신 주체(P1)에게 전송한 상기 큐빗 집합의 인코딩 시에 이용된 인코딩 베이시스가 상기 제5 통신 주체(P5)로부터 수신한 상기 제4 예측 베이시스와 일치하는지 판단한다.

[0070] 모두 설명하지 않았으나, 상기 제2 통신 주체(P2) 내지 상기 제5 통신 주체(P5)도 상기 제1 통신 주체(P1)와 같은 방식으로 상기 예측 베이시스와 상기 인코딩 베이시스의 일치 여부의 판단을 받아볼 수 있다.

[0071] 상기 N개의 통신 주체들이 다른 N-1 통신 주체의 인코딩 베이시스들을 예측하여 맞춘 개수를 기초로 상기 N개의 통신 주체들의 순위를 결정한다. 상기 N개의 통신 주체들이 다른 N-1 통신 주체의 인코딩 베이시스들을 예측하여 맞춘 개수의 최대값은 N-1이고, 상기 N개의 통신 주체들이 다른 N-1 통신 주체의 인코딩 베이시스들을 예측하여 맞춘 개수의 최소값은 0이다.

[0072] 상기 N개의 통신 주체들 각각은 상기 N-1개의 통신 주체들에게 상기 N-1개의 큐빗 집합 내의 상기 큐빗들의 상태 시퀀스를 각각 전송할 수 있다. 상기 예측 베이시스와 상기 인코딩 베이시스의 일치 여부 및 상기 상태 시퀀스를 수신한 통신 주체는 상기 수신한 예측 베이시스와 상기 인코딩 베이시스의 일치 여부의 결과가 정확한 지를 상기 수신한 상태 시퀀스를 이용하여 검증할 수 있다. 따라서, 상기 예측 베이시스와 상기 인코딩 베이시스의 일치 여부를 알려주는 통신 주체는 속임수(cheat)를 사용할 수 없다.

[0073] 예를 들어, 상기 제2 통신 주체(P2)는 상기 제2 통신 주체(P2)가 상기 제1 통신 주체(P1)에게 전송한 상기 큐빗 집합의 인코딩 시에 이용된 인코딩 베이시스가 상기 제1 통신 주체(P1)로부터 수신한 상기 제1 예측 베이시스와 일치하는지 여부와 상기 제2 통신 주체(P2)가 상기 제1 통신 주체(P1)에게 전송한 상기 큐빗 집합의 상태 시퀀스를 상기 제1 통신 주체(P1)에게 전송한다. 상기 제1 통신 주체(P1)는 상기 큐빗 집합의 상태 시퀀스를 이용하여 상기 제2 통신 주체(P2)가 통지한 상기 인코딩 베이시스와 상기 제1 예측 베이시스의 일치 여부를 검증할 수 있다.

[0074] 예를 들어, 상기 제1 통신 주체(P1)는 상기 제3 통신 주체(P3)가 생성 및 인코딩하여 상기 제1 통신 주체(P1)에게 전송한 상기 큐빗 집합의 상태 시퀀스를 상기 제3 통신 주체(P3)로부터 수신한다. 예를 들어, 상기 제1 통신 주체(P1)는 상기 제4 통신 주체(P4)가 생성 및 인코딩하여 상기 제1 통신 주체(P1)에게 전송한 상기 큐빗 집합의 상태 시퀀스를 상기 제4 통신 주체(P4)로부터 수신한다. 예를 들어, 상기 제1 통신 주체(P1)는 상기 제5 통신 주체(P5)가 생성 및 인코딩하여 상기 제1 통신 주체(P1)에게 전송한 상기 큐빗 집합의 상태 시퀀스를 상기 제5 통신 주체(P5)로부터 수신한다.

[0075] 모두 설명하지 않았으나, 상기 제2 통신 주체(P2) 내지 상기 제5 통신 주체(P5)도 상기 제1 통신 주체(P1)와 같은 방식으로 상기 큐빗 집합의 상태 시퀀스를 받아볼 수 있다.

[0076] 상기 N개의 통신 주체들 간의 순위를 결정하는 단계는 상기 N개의 통신 주체들 각각이 상기 N-1개의 통신 주체들의 상기 인코딩 베이시스들을 예측하여 맞춘 개수를 기초로 상기 N개의 통신 주체들의 제1 리스트를 생성하는 단계를 포함할 수 있다.

[0077] 상기 제1 리스트 내에서 상기 인코딩 베이시스들을 예측하여 맞춘 개수가 동일한 통신 주체들 간에는 양자 추첨을 재수행할 수 있다. 상기 제1 리스트 및 상기 양자 추첨 재수행 결과를 기초로 제2 리스트를 생성할 수 있다.

[0078] 본 실시예에서, 상기 N개의 통신 주체들은 서로 원거리에 배치될 수 있다. 즉, 상기 양자 통신 시스템 내에서 각 통신 주체들이 서로 원거리에 있는 경우라도 별도의 중재 통신 주체 없이 복수의 통신 주체들 간에 공정하게 순위를 정할 수 있다.

[0079] 또한, 상기 양자 추첨 방법(순위를 가리는 방법)을 이용한 양자 통신 방법은 상기 N개의 통신 주체들 사이의 상기 순위를 기초로 자원을 분배하는 단계를 더 포함한다.

[0080] 상기 N개의 통신 주체들의 순위는 공정성이 보장되기 때문에 상기 공정한 순위를 기초로 상기 N개의 통신 주체들 간에 자원을 공정하게 분배할 수 있다.

[0081] 예를 들어, 상기 양자 추첨 방법을 이용하여 양자 통신 시스템 내의 통신 주체들 간에 통신 우선 순위(priority)를 제공할 수 있다. 예를 들어, 상기 제1 내지 제5 통신 주체 중 제1 통신 주체의 순위가 가장 높은 경우, 상기 제1 통신 주체가 다른 통신 주체들에게 우선적으로 자료를 전송하도록 할 수 있다.

[0082] 예를 들어, 상기 양자 추첨 방법을 이용하여 양자 통신 시스템 내의 통신 주체들 간에 자원 선택의 우선 순위(priority)를 제공할 수 있다. 예를 들어, 상기 제1 내지 제5 통신 주체 중 제1 통신 주체의 순위가 가장 높은 경우, 상기 제1 통신 주체가 배분 가능한 자원 중 본인에게 유리한 자원을 먼저 선택할 수 있다.

[0083] 예를 들어, 상기 양자 추첨 방법을 이용하여 양자 통신 시스템 내의 통신 주체들 간에 상금을 배분하는 게임을 설계할 수 있다. 예를 들어, 5개의 통신 주체 중 1위에게 일만 달러를 2위에게 오천 달러를 제공하는 게임이 있

을 때, 상기 제1 내지 제5 통신 주체 중 상기 제1 통신 주체의 순위가 1위라면 상기 제1 통신 주체가 일만 달러를 얻고, 상기 제3 통신 주체의 순위가 2위 라면 상기 제3 통신 주체가 오천 달러를 얻도록 할 수 있다.

[0084] 상기 양자 추첨 방식은 양자 통신에 내재된 공정성을 기초로 상기 양자 통신 시스템 내에 있는 통신 주체들 간에 순위를 매길 필요가 있는 다양한 양자 통신 시스템에 적용될 수 있다.

[0085] 도 2a는 도 1의 양자 통신 시스템에서 큐빗의 제1 베이시스를 나타내는 개념도이다. 도 2b는 도 1의 양자 통신 시스템에서 상기 큐빗의 제2 베이시스를 나타내는 개념도이다. 도 3은 도 1의 양자 통신 시스템에서 상기 큐빗의 제1 베이시스 및 제2 베이시스에 따른 제1 상태 및 제2 상태를 나타내는 표이다.

[0086] 도 1 내지 도 3을 참조하면, 상기 양자 통신 시스템에서 상기 통신 주체들 간에 주고 받는 큐빗 집합은 각각 M개의 큐빗을 포함할 수 있다.

[0087] 예를 들어, 상기 큐빗은 제1 상태, 제2 상태 및 제3 상태를 가질 수 있다. 상기 제1 상태는 $|0\rangle$ 이고, 상기 제2 상태는 $|1\rangle$ 일 수 있다. 상기 제3 상태는 $a|0\rangle+b|1\rangle$ 이고, 상기 a^2은 상기 큐빗의 상태가 $|0\rangle$ 일 확률이며, 상기 b^2은 상기 큐빗의 상태가 $|1\rangle$ 일 확률일 수 있다.

[0088] 이 때, a와 b의 관계는 $|a|^2+|b|^2=1$로 정의될 수 있다.

[0089] 예를 들어, 상기 큐빗은 광자(Photon)에 의해 전송될 수 있다. 상기 큐빗은 제1 베이시스 및 제2 베이시스를 이용하여 인코딩 및 측정될 수 있다. 예를 들어, 상기 큐빗이 광자(Photon)에 의해 전송될 때, 상기 제1 베이시스는 수직 수평 베이시스(RECTILINEAR BASIS)일 수 있고, 상기 제2 베이시스는 대각 베이시스(DIAGONAL BASIS)일 수 있다.

[0090] 상기 큐빗이 상기 제1 베이시스(수직 수평 베이시스)에 의해 인코딩 및 측정될 때, 상기 큐빗이 수평 방향의 편광을 가지면 상기 큐빗은 0이고, 상기 큐빗이 수직 방향의 편광을 가지면 상기 큐빗은 1일 수 있다.

[0091] 상기 큐빗이 상기 제2 베이시스(대각 베이시스)에 의해 인코딩 및 측정될 때, 상기 큐빗이 제1 대각 방향의 편광을 가지면 상기 큐빗은 0이고, 상기 큐빗이 제2 대각 방향의 편광을 가지면 상기 큐빗은 1일 수 있다. 상기 제1 대각 방향은 좌하부와 우상부를 연결하는 방향일 수 있다. 상기 제2 대각 방향은 좌상부와 우하부를 연결하는 방향일 수 있다.

[0092] 이와는 달리, 상기 큐빗은 전자(Electron)에 의해 전송될 수 있고, 이 때 상기 제1 상태 및 상기 제2 상태는 spin up 및 spin down으로 표현될 수 있다.

[0093] 도 4는 도 1의 양자 통신 시스템에서 제1 통신 주체 및 제2 통신 주체의 동작의 일례를 나타내는 표이다. 도 5는 도 1의 양자 통신 시스템에서 제1 통신 주체 및 제4 통신 주체의 동작의 일례를 나타내는 표이다.

[0094] 도 4에서는 상기 제1 통신 주체(P1)가 상기 제2 통신 주체(P2)에게 인코딩된 큐빗 집합을 전송하고, 상기 제2 통신 주체(P2)가 상기 제1 통신 주체(P1)가 전송한 큐빗 집합의 인코딩 베이시스를 맞게 예측한 경우를 예시한다.

[0095] 도 1 내지 도 4를 참조하면, 상기 제1 통신 주체(P1)는 15개의 큐빗을 갖는 제1 큐빗 집합을 생성한다. 상기 제1 큐빗 집합의 각 큐빗은 0 또는 1의 상태를 갖고, 상기 제1 큐빗 집합의 상태 시퀀스(15개)는 "101001110101100"이다. 상기 제1 큐빗 집합은 수평 수직 베이시스(RECTILINEAR)로 인코딩된다.

[0096] 도 3 및 도 4에서 보듯이, 상기 제1 큐빗 집합 내의 "1"이 상기 수평 수직 베이시스(RECTILINEAR)에 의해 인코딩되는 경우 상기 큐빗은 수직 방향의 편광 방향을 갖게 되고, 상기 제1 큐빗 집합 내의 "0"이 상기 수평 수직 베이시스(RECTILINEAR)에 의해 인코딩되는 경우 상기 큐빗은 수평 방향의 편광 방향을 갖게 된다.

[0097] 상기 제1 통신 주체(P1)가 상기 수평 수직 베이시스를 이용하여 "0"을 광자를 통해 보내게 되면, 상기 제2 통신 주체(P2)는 상기 수평 방향의 편광 방향을 갖는 광자를 수신하게 된다.

[0098] 상기 제1 통신 주체(P1)가 상기 수평 수직 베이시스를 이용하여 "1"을 광자를 통해 보내게 되면, 상기 제2 통신 주체(P2)는 상기 수직 방향의 편광 방향을 갖는 광자를 수신하게 된다.

[0099] 상기 제2 통신 주체(P2)는 각 비트마다 랜덤 베이시스를 이용하여 상기 큐빗을 측정하게 된다. 도 4 내에서 R은 수평 수직 베이시스를 의미하고, D는 대각 베이시스를 의미한다.

[0100] 상기 제2 통신 주체(P2)가 상기 수평 방향의 편광 방향을 갖는 광자를 상기 수평 수직 베이시스를 이용하여 측

정하게 되면, 상기 제2 통신 주체(P2)는 0의 값을 얻는다.

[0101] 상기 제2 통신 주체(P2)가 상기 수직 방향의 편광 방향을 갖는 광자를 상기 수평 수직 베이시스를 이용하여 측정하게 되면, 상기 제2 통신 주체(P2)는 1의 값을 얻는다.

[0102] 이와 같이, 상기 제1 통신 주체(P1)가 인코딩 시에 사용한 베이시스(R)와 상기 제2 통신 주체(P2)가 측정 시에 사용한 베이시스(R)가 서로 일치하는 경우, 상기 제2 통신 주체(P2)가 측정한 상기 큐빗의 상태 값은 상기 제1 통신 주체(P1)의 상기 큐빗의 상태와 일치하게 된다.

[0103] 상기 제2 통신 주체(P2)가 상기 수평 방향의 편광 방향을 갖는 광자를 상기 대각 베이시스를 이용하여 측정하게 되면, 상기 제2 통신 주체(P2)는 50%의 확률로 0의 값을 얻거나 1의 값을 얻는다.

[0104] 상기 제2 통신 주체(P2)가 상기 수직 방향의 편광 방향을 갖는 광자를 상기 대각 베이시스를 이용하여 측정하게 되면, 상기 제2 통신 주체(P2)는 50%의 확률로 0의 값을 얻거나 1의 값을 얻는다.

[0105] 이와 같이, 상기 제1 통신 주체(P1)가 인코딩 시에 사용한 베이시스(R)와 상기 제2 통신 주체(P2)가 측정 시에 사용한 베이시스(D)가 서로 일치하지 않는 경우, 상기 제2 통신 주체(P2)가 측정한 상기 큐빗의 상태 값은 상기 제1 통신 주체(P1)의 상기 큐빗의 상태와 일치할 수도 있고 일치하지 않을 수도 있다. 상기 제1 통신 주체(P1)가 인코딩 시에 사용한 베이시스(R)와 상기 제2 통신 주체(P2)가 측정 시에 사용한 베이시스(D)가 서로 일치하지 않는 경우, 상기 제2 통신 주체(P2)가 측정한 상기 큐빗의 상태 값은 부정확한 값이라 할 수 있다.

[0106] 도 4에서 상기 제1 통신 주체(P1)는 "101001110101100"의 상태 시퀀스(P1's BIT STRING)를 갖는 제1 큐빗 집합을 수평 수직 베이시스(P1's RANDOM BASIS - RECTILINEAR)로 인코딩하여 상기 제2 통신 주체(P2)에게 전송한다.

[0107] 상기 제2 통신 주체(P2)는 상기 큐빗 집합 중 상태 값이 0인 제11 비트 및 제15 비트를 수평 수직 베이시스(R)를 이용하여 측정하였고 상기 제2 통신 주체(P2)가 측정한 상태 값(P2's RECTILINEAR TABLE)은 0이 되어 상기 제1 통신 주체(P1)가 전송한 큐빗의 상태 값과 일치한다.

[0108] 상기 제2 통신 주체(P2)는 상기 큐빗 집합 중 상태 값이 1인 제1 비트 및 제6 비트를 수평 수직 베이시스(R)를 이용하여 측정하였고 상기 제2 통신 주체(P2)가 측정한 상태 값(P2's RECTILINEAR TABLE)은 1이 되어 상기 제1 통신 주체(P1)가 전송한 큐빗의 상태 값과 일치한다.

[0109] 상기 제2 통신 주체(P2)는 상기 큐빗 집합 중 상태 값이 0인 제2 비트 및 제4 비트를 대각 베이시스(D)를 이용하여 측정하였고 상기 제2 통신 주체(P2)가 측정한 상태 값(P2's DIAGONAL TABLE)은 각각 0과 1이 되어 상기 제1 통신 주체(P1)가 전송한 큐빗의 상태 값과 일치할 때도 있고 일치하지 않을 때도 있다.

[0110] 상기 제2 통신 주체(P2)는 상기 큐빗 집합 중 상태 값이 1인 제10 비트 및 제13 비트를 대각 베이시스(D)를 이용하여 측정하였고 상기 제2 통신 주체(P2)가 측정한 상태 값(P2's DIAGONAL TABLE)은 각각 1과 0이 되어 상기 제1 통신 주체(P1)가 전송한 큐빗의 상태 값과 일치할 때도 있고 일치하지 않을 때도 있다.

[0111] 도 4에서 상기 제2 통신 주체(P2)는 상기 제1 통신 주체(P1)의 큐빗 집합이 인코딩 될 때 이용된 인코딩 베이시스를 수평 수직 베이시스(P2's GUESS - RECTILINEAR)로 예측하였다. 상기 제2 통신 주체(P2)는 상기 예측 베이시스를 상기 제1 통신 주체(P1)에게 전송한다.

[0112] 상기 제1 통신 주체(P1)는 상기 제2 통신 주체(P2)에게 전송한 큐빗 집합의 인코딩에 이용된 베이시스(P1's RANDOM BASIS - RECTILINEAR)와 상기 제2 통신 주체(P2)의 예측 베이시스(P2's GUESS - RECTILINEAR)가 일치하는지를 판단한다. 본 실시예에서, 상기 제1 통신 주체(P1)는 상기 제2 통신 주체(P2)에게 전송한 큐빗 집합의 인코딩에 이용된 베이시스(P1's RANDOM BASIS - RECTILINEAR)와 상기 제2 통신 주체(P2)의 예측 베이시스(P2's GUESS - RECTILINEAR)가 일치한다. 따라서, 상기 제1 통신 주체(P1)는 상기 제2 통신 주체(P2)에게 "YOU ARE RIGHT"의 메시지(P1's REPLY)를 전송한다.

[0113] 또한, 상기 제1 통신 주체(P1)는 상기 제2 통신 주체(P2)에게 상기 큐빗 집합 내의 상기 큐빗들의 상태 시퀀스 "101001110101100"(P1's ORIGINAL BIT STRING TO CERTIFY)를 전송한다. 이로 인해, 상기 제2 통신 주체(P2)는 상기 제1 통신 주체(P1)가 속임수를 사용하지 않았는지 확인이 가능하다.

[0114] 도 5에서는 상기 제1 통신 주체(P1)가 상기 제4 통신 주체(P4)에게 인코딩된 큐빗 집합을 전송하고, 상기 제4 통신 주체(P4)가 상기 제1 통신 주체(P1)가 전송한 큐빗 집합의 인코딩 베이시스를 틀리게 예측한 경우를 예시한다.

[0115] 도 1 내지 도 3 및 도 5를 참조하면, 상기 제1 통신 주체(P1)는 15개의 큐빗을 갖는 제3 큐빗 집합을 생성한다. 상기 제3 큐빗 집합의 각 큐빗은 0 또는 1의 상태를 갖고, 상기 제3 큐빗 집합의 상태 시퀀스(15개)는 "110100011010001"이다. 상기 제3 큐빗 집합은 대각 베이시스(DIAGONAL)로 인코딩된다.

[0116] 도 3 및 도 5에서 보듯이, 상기 제3 큐빗 집합 내의 "0"이 상기 대각 베이시스(DIAGONAL)에 의해 인코딩되는 경우 상기 큐빗은 제1 대각 방향의 편광 방향을 갖게 되고, 상기 제3 큐빗 집합 내의 "1"이 상기 대각 베이시스(RECTILINEAR)에 의해 인코딩되는 경우 상기 큐빗은 제2 대각 방향의 편광 방향을 갖게 된다.

[0117] 상기 제1 통신 주체(P1)가 상기 대각 베이시스를 이용하여 "0"을 광자를 통해 보내게 되면, 상기 제4 통신 주체(P4)는 상기 제1 대각 방향의 편광 방향을 갖는 광자를 수신하게 된다.

[0118] 상기 제1 통신 주체(P1)가 상기 대각 베이시스를 이용하여 "1"을 광자를 통해 보내게 되면, 상기 제4 통신 주체(P4)는 상기 제2 대각 방향의 편광 방향을 갖는 광자를 수신하게 된다.

[0119] 상기 제4 통신 주체(P4)는 각 비트마다 랜덤 베이시스를 이용하여 상기 큐빗을 측정하게 된다. 도 4 내에서 R은 수평 수직 베이시스를 의미하고, D는 대각 베이시스를 의미한다.

[0120] 상기 제4 통신 주체(P4)가 상기 제1 대각 방향의 편광 방향을 갖는 광자를 상기 대각 베이시스를 이용하여 측정하게 되면, 상기 제4 통신 주체(P4)는 0의 값을 얻는다.

[0121] 상기 제4 통신 주체(P4)가 상기 제2 대각 방향의 편광 방향을 갖는 광자를 상기 대각 베이시스를 이용하여 측정하게 되면, 상기 제4 통신 주체(P4)는 1의 값을 얻는다.

[0122] 이와 같이, 상기 제1 통신 주체(P1)가 인코딩 시에 사용한 베이시스(D)와 상기 제4 통신 주체(P4)가 측정 시에 사용한 베이시스(D)가 서로 일치하는 경우, 상기 제4 통신 주체(P4)가 측정한 상기 큐빗의 상태 값은 상기 제1 통신 주체(P1)의 상기 큐빗의 상태와 일치하게 된다.

[0123] 상기 제4 통신 주체(P4)가 상기 제1 대각 방향의 편광 방향을 갖는 광자를 상기 수평 수직 베이시스를 이용하여 측정하게 되면, 상기 제4 통신 주체(P4)는 50%의 확률로 0의 값을 얻거나 1의 값을 얻는다.

[0124] 상기 제4 통신 주체(P4)가 상기 제2 대각 방향의 편광 방향을 갖는 광자를 상기 수평 수직 베이시스를 이용하여 측정하게 되면, 상기 제4 통신 주체(P4)는 50%의 확률로 0의 값을 얻거나 1의 값을 얻는다.

[0125] 이와 같이, 상기 제1 통신 주체(P1)가 인코딩 시에 사용한 베이시스(D)와 상기 제4 통신 주체(P4)가 측정 시에 사용한 베이시스(R)가 서로 일치하지 않는 경우, 상기 제4 통신 주체(P4)가 측정한 상기 큐빗의 상태 값은 상기 제1 통신 주체(P1)의 상기 큐빗의 상태와 일치할 수도 있고 일치하지 않을 수도 있다. 상기 제1 통신 주체(P1)가 인코딩 시에 사용한 베이시스(D)와 상기 제4 통신 주체(P4)가 측정 시에 사용한 베이시스(R)가 서로 일치하지 않는 경우, 상기 제4 통신 주체(P4)가 측정한 상기 큐빗의 상태 값은 부정확한 값이라 할 수 있다.

[0126] 도 5에서 상기 제1 통신 주체(P1)는 "110100011010001"의 상태 시퀀스(P1's BIT STRING)를 갖는 제3 큐빗 집합을 대각 베이시스(P1's RANDOM BASIS - DIAGONAL)로 인코딩하여 상기 제4 통신 주체(P4)에게 전송한다.

[0127] 상기 제4 통신 주체(P4)는 상기 큐빗 집합 중 상태 값이 0인 제5 비트 및 제13 비트를 대각 베이시스(D)를 이용하여 측정하였고 상기 제4 통신 주체(P4)가 측정한 상태 값(P4's DIAGONAL TABLE)은 0이 되어 상기 제1 통신 주체(P1)가 전송한 큐빗의 상태 값과 일치한다.

[0128] 상기 제4 통신 주체(P4)는 상기 큐빗 집합 중 상태 값이 1인 제1 비트 및 제9 비트를 대각 베이시스(D)를 이용하여 측정하였고 상기 제4 통신 주체(P4)가 측정한 상태 값(P4's DIAGONAL TABLE)은 1이 되어 상기 제1 통신 주체(P1)가 전송한 큐빗의 상태 값과 일치한다.

[0129] 상기 제4 통신 주체(P4)는 상기 큐빗 집합 중 상태 값이 0인 제3 비트 및 제7 비트를 수평 수직 베이시스(R)를 이용하여 측정하였고 상기 제4 통신 주체(P4)가 측정한 상태 값(P4's RECTILINEAR TABLE)은 각각 0과 1이 되어 상기 제1 통신 주체(P1)가 전송한 큐빗의 상태 값과 일치할 때도 있고 일치하지 않을 때도 있다.

[0130] 상기 제4 통신 주체(P4)는 상기 큐빗 집합 중 상태 값이 1인 제11 비트 및 제15 비트를 수평 수직 베이시스(R)를 이용하여 측정하였고 상기 제4 통신 주체(P4)가 측정한 상태 값(P4's RECTILINEAR TABLE)은 각각 0과 1이 되어 상기 제1 통신 주체(P1)가 전송한 큐빗의 상태 값과 일치할 때도 있고 일치하지 않을 때도 있다.

[0131] 도 5에서 상기 제4 통신 주체(P4)는 상기 제1 통신 주체(P1)의 큐빗 집합이 인코딩 될 때 이용된 인코딩 베이시스를 수평 수직 베이시스(P4's GUESS - RECTILINEAR)로 예측하였다. 상기 제4 통신 주체(P4)는 상기 예측 베이

시스를 상기 제1 통신 주체(P1)에게 전송한다.

[0132] 상기 제1 통신 주체(P1)는 상기 제4 통신 주체(P4)에게 전송한 큐빗 집합의 인코딩에 이용된 베이시스(P1's RANDOM BASIS - DIAGONAL)와 상기 제4 통신 주체(P4)의 예측 베이시스(P4's GUESS - RECTILINEAR)가 일치하는지 여부를 판단한다. 본 실시예에서는 상기 제1 통신 주체(P1)는 상기 제4 통신 주체(P4)에게 전송한 큐빗 집합의 인코딩에 이용된 베이시스(P1's RANDOM BASIS - DIAGONAL)와 상기 제4 통신 주체(P4)의 예측 베이시스(P4's GUESS - RECTILINEAR)가 일치하지 않는다. 따라서, 상기 제1 통신 주체(P1)는 상기 제4 통신 주체(P4)에게 "YOU ARE WRONG"의 메시지(P1's REPLY)를 전송한다.

[0133] 또한, 상기 제1 통신 주체(P1)는 상기 제4 통신 주체(P4)에게 상기 큐빗 집합 내의 상기 큐빗들의 상태 시퀀스 "110100011010001"(P1's ORIGINAL BIT STRING TO CERTIFY)를 전송한다. 이로 인해, 상기 제4 통신 주체(P4)는 상기 제1 통신 주체(P1)가 속임수를 사용하지 않았는지 확인이 가능하다.

[0134] 도 6a는 도 1의 양자 통신 시스템에서 제1 통신 주체가 다른 통신 주체들에게 통지하는 정보의 일례를 나타내는 표이다. 도 6b는 도 1의 양자 통신 시스템에서 제2 통신 주체가 다른 통신 주체들에게 통지하는 정보의 일례를 나타내는 표이다. 도 6c는 도 1의 양자 통신 시스템에서 제3 통신 주체가 다른 통신 주체들에게 통지하는 정보의 일례를 나타내는 표이다. 도 6d는 도 1의 양자 통신 시스템에서 제4 통신 주체가 다른 통신 주체들에게 통지하는 정보의 일례를 나타내는 표이다. 도 6e는 도 1의 양자 통신 시스템에서 제5 통신 주체가 다른 통신 주체들에게 통지하는 정보의 일례를 나타내는 표이다. 도 7은 도 1의 양자 통신 시스템에서 예측 베이시스와 인코딩 베이시스의 일치 여부의 개수를 기초로 생성되는 제1 리스트이다. 도 8은 도 1의 양자 통신 시스템에서 예측 베이시스와 인코딩 베이시스의 일치 여부의 개수를 기초로 생성되는 제2 리스트이다.

[0135] 도 6a는 상기 제1 통신 주체(P1)가 상기 큐빗 집합을 실제로 인코딩한 인코딩 베이시스와 다른 통신 주체들(P2 내지 P5)의 예측 베이시스의 일치 여부에 대한 예시를 나타내었다. 상기 제2 통신 주체(P2)는 상기 제2 통신 주체(P2)가 상기 제1 통신 주체(P1)로부터 수신한 큐빗 집합의 인코딩 베이시스를 맞게 예측하였다. 상기 제3 통신 주체(P3)는 상기 제3 통신 주체(P3)가 상기 제1 통신 주체(P1)로부터 수신한 큐빗 집합의 인코딩 베이시스를 맞게 예측하였다. 상기 제4 통신 주체(P4)는 상기 제4 통신 주체(P4)가 상기 제1 통신 주체(P1)로부터 수신한 큐빗 집합의 인코딩 베이시스를 틀리게 예측하였다. 상기 제5 통신 주체(P5)는 상기 제5 통신 주체(P5)가 상기 제1 통신 주체(P1)로부터 수신한 큐빗 집합의 인코딩 베이시스를 틀리게 예측하였다.

[0136] 도 6b는 상기 제2 통신 주체(P2)가 상기 큐빗 집합을 실제로 인코딩한 인코딩 베이시스와 다른 통신 주체들(P1, P3, P4, P5)의 예측 베이시스의 일치 여부에 대한 예시를 나타내었다. 상기 제1 통신 주체(P1)는 상기 제1 통신 주체(P1)가 상기 제2 통신 주체(P2)로부터 수신한 큐빗 집합의 인코딩 베이시스를 맞게 예측하였다. 상기 제3 통신 주체(P3)는 상기 제3 통신 주체(P3)가 상기 제2 통신 주체(P2)로부터 수신한 큐빗 집합의 인코딩 베이시스를 맞게 예측하였다. 상기 제4 통신 주체(P4)는 상기 제4 통신 주체(P4)가 상기 제2 통신 주체(P2)로부터 수신한 큐빗 집합의 인코딩 베이시스를 틀리게 예측하였다. 상기 제5 통신 주체(P5)는 상기 제5 통신 주체(P5)가 상기 제2 통신 주체(P2)로부터 수신한 큐빗 집합의 인코딩 베이시스를 틀리게 예측하였다.

[0137] 도 6c는 상기 제3 통신 주체(P3)가 상기 큐빗 집합을 실제로 인코딩한 인코딩 베이시스와 다른 통신 주체들(P1, P2, P4, P5)의 예측 베이시스의 일치 여부에 대한 예시를 나타내었다. 상기 제1 통신 주체(P1)는 상기 제1 통신 주체(P1)가 상기 제3 통신 주체(P3)로부터 수신한 큐빗 집합의 인코딩 베이시스를 맞게 예측하였다. 상기 제2 통신 주체(P2)는 상기 제2 통신 주체(P2)가 상기 제3 통신 주체(P3)로부터 수신한 큐빗 집합의 인코딩 베이시스를 맞게 예측하였다. 상기 제4 통신 주체(P4)는 상기 제4 통신 주체(P4)가 상기 제3 통신 주체(P3)로부터 수신한 큐빗 집합의 인코딩 베이시스를 틀리게 예측하였다. 상기 제5 통신 주체(P5)는 상기 제5 통신 주체(P5)가 상기 제3 통신 주체(P3)로부터 수신한 큐빗 집합의 인코딩 베이시스를 틀리게 예측하였다.

[0138] 도 6d는 상기 제4 통신 주체(P4)가 상기 큐빗 집합을 실제로 인코딩한 인코딩 베이시스와 다른 통신 주체들(P1, P2, P3, P5)의 예측 베이시스의 일치 여부에 대한 예시를 나타내었다. 상기 제1 통신 주체(P1)는 상기 제1 통신 주체(P1)가 상기 제4 통신 주체(P4)로부터 수신한 큐빗 집합의 인코딩 베이시스를 맞게 예측하였다. 상기 제2 통신 주체(P2)는 상기 제2 통신 주체(P2)가 상기 제4 통신 주체(P4)로부터 수신한 큐빗 집합의 인코딩 베이시스를 틀리게 예측하였다. 상기 제3 통신 주체(P3)는 상기 제3 통신 주체(P3)가 상기 제4 통신 주체(P4)로부터 수신한 큐빗 집합의 인코딩 베이시스를 틀리게 예측하였다. 상기 제5 통신 주체(P5)는 상기 제5 통신 주체(P5)가 상기 제4 통신 주체(P4)로부터 수신한 큐빗 집합의 인코딩 베이시스를 틀리게 예측하였다.

[0139] 도 6e는 상기 제5 통신 주체(P5)가 상기 큐빗 집합을 실제로 인코딩한 인코딩 베이시스와 다른 통신 주체들(P1

내지 P4)의 예측 베이시스의 일치 여부에 대한 예시를 나타내었다. 상기 제1 통신 주체(P1)는 상기 제1 통신 주체(P1)가 상기 제5 통신 주체(P5)로부터 수신한 큐빗 집합의 인코딩 베이시스를 맞게 예측하였다. 상기 제2 통신 주체(P2)는 상기 제2 통신 주체(P2)가 상기 제5 통신 주체(P5)로부터 수신한 큐빗 집합의 인코딩 베이시스를 맞게 예측하였다. 상기 제3 통신 주체(P3)는 상기 제3 통신 주체(P3)가 상기 제5 통신 주체(P5)로부터 수신한 큐빗 집합의 인코딩 베이시스를 맞게 예측하였다. 상기 제5 통신 주체(P5)는 상기 제5 통신 주체(P5)가 상기 제5 통신 주체(P5)로부터 수신한 큐빗 집합의 인코딩 베이시스를 맞게 예측하였다.

[0140] 도 7(SORTED LIST)에서 보듯이, 상기 제1 통신 주체(P1)는 다른 통신 주체들(P2 내지 P5)의 인코딩 베이시스를 모두 맞게 예측하여 4점을 얻어 1위에 배치되었다. 상기 제2 통신 주체(P2)는 다른 통신 주체들(P1, P3, P4, P5)의 인코딩 베이시스 중 3개를 맞게 예측하여 3점을 얻어 2위에 배치되었다. 상기 제3 통신 주체(P3)는 다른 통신 주체들(P1, P2, P4, P5)의 인코딩 베이시스 중 3개를 맞게 예측하여 3점을 얻어 상기 제2 통신 주체(P2)와 함께 공동 2위에 배치되었다. 상기 제4 통신 주체(P4)는 다른 통신 주체들(P1, P2, P3, P5)의 인코딩 베이시스 중 1개를 맞게 예측하여 1점을 얻어 4위에 배치되었다. 상기 제5 통신 주체(P5)는 다른 통신 주체들(P1 내지 P4)의 인코딩 베이시스를 모두 틀리게 예측하여 0점을 얻어 5위에 배치되었다.

[0141] 본 발명의 일 실시예에서, 도 7의 공동 2위에 해당하는 제2 통신 주체(P2) 및 제3 통신 주체(P3)의 순위를 결정하기 위해 상기 제2 통신 주체(P2) 및 상기 제3 통신 주체(P3) 간에 양자 추첨을 재수행할 수 있다. 이 때, 상기 양자 추첨은 공동 순위를 갖는 통신 주체들만 수행할 수 있다. 이와는 달리, 상기 양자 추첨은 모든 통신 주체들이 함께 수행하고, 상기 공동 순위를 갖는 통신 주체들의 순위만을 가릴 수도 있다.

[0142] 도 8에서는 상기 제2 통신 주체(P2) 및 상기 제3 통신 주체(P3) 간에 양자 추첨을 재수행하여 상기 제2 통신 주체(P2)는 상기 제3 통신 주체(P3)의 인코딩 베이시스를 맞추지 못하고 상기 제3 통신 주체(P3)는 상기 제2 통신 주체(P2)의 인코딩 베이시스를 맞춘 경우를 예시하였다.

[0143] 따라서, 최종적으로 상기 제3 통신 주체(P3)는 2위가 되고, 상기 제2 통신 주체(P2)는 3위가 되었다.

[0144] 본 발명의 일 실시예에서, 상기 양자 통신 시스템은 서로 통신하는 제1 통신 주체, 제2 통신 주체 및 제3 통신 주체를 포함할 수 있다. (N이 3인 경우)

[0145] 상기 제1 통신 주체는 제1 큐빗 집합 및 제2 큐빗 집합을 생성하고, 상기 제1 큐빗 집합 및 상기 제2 큐빗 집합을 제1 베이시스 및 제2 베이시스를 이용하여 인코딩하며, 상기 인코딩된 제1 큐빗 집합을 상기 제2 통신 주체에게 전송하고, 상기 인코딩된 제2 큐빗 집합을 상기 제3 통신 주체에게 전송한다.

[0146] 상기 제2 통신 주체는 제3 큐빗 집합 및 제4 큐빗 집합을 생성하고, 상기 제3 큐빗 집합 및 상기 제4 큐빗 집합을 상기 제1 베이시스 및 상기 제2 베이시스를 이용하여 인코딩하며, 상기 인코딩된 제3 큐빗 집합을 상기 제1 통신 주체에게 전송하고, 상기 인코딩된 제4 큐빗 집합을 상기 제3 통신 주체에게 전송한다.

[0147] 상기 제3 통신 주체는 제5 큐빗 집합 및 제6 큐빗 집합을 생성하고, 상기 제5 큐빗 집합 및 상기 제6 큐빗 집합을 상기 제1 베이시스 및 상기 제2 베이시스를 이용하여 인코딩하며, 상기 인코딩된 제5 큐빗 집합을 상기 제1 통신 주체에게 전송하고, 상기 인코딩된 제6 큐빗 집합을 상기 제2 통신 주체에게 전송한다.

[0148] 상기 제1 통신 주체는 상기 제3 큐빗 집합이 인코딩될 때 이용된 베이시스를 예측하여 상기 제2 통신 주체에게 전송하며, 상기 제5 큐빗 집합이 인코딩될 때 이용된 베이시스를 예측하여 상기 제3 통신 주체에게 전송한다.

[0149] 상기 제2 통신 주체는 상기 제1 큐빗 집합이 인코딩될 때 이용된 베이시스를 예측하여 상기 제1 통신 주체에게 전송하며, 상기 제6 큐빗 집합이 인코딩될 때 이용된 베이시스를 예측하여 상기 제3 통신 주체에게 전송한다.

[0150] 상기 제3 통신 주체는 상기 제2 큐빗 집합이 인코딩될 때 이용된 베이시스를 예측하여 상기 제1 통신 주체에게 전송하며, 상기 제4 큐빗 집합이 인코딩될 때 이용된 베이시스를 예측하여 상기 제2 통신 주체에게 전송한다. 상기 제1 내지 제6 큐빗 집합들 각각은 M개(M은 2 이상의 자연수)의 큐빗들을 포함한다.

[0151] 본 발명의 일 실시예에 있어서, 상기 양자 통신 시스템은 상기 제1 통신 주체, 상기 제2 통신 주체 및 상기 제3 통신 주체와 통신하는 제4 통신 주체를 더 포함할 수 있다. (N이 4인 경우)

[0152] 상기 제1 통신 주체는 제7 큐빗 집합을 생성 및 인코딩하여, 상기 인코딩된 상기 제7 큐빗 집합을 상기 제4 통신 주체에게 전송하고, 상기 제2 통신 주체는 제8 큐빗 집합을 생성 및 인코딩하여, 상기 인코딩된 상기 제8 큐빗 집합을 상기 제4 통신 주체에게 전송하며, 상기 제3 통신 주체는 제9 큐빗 집합을 생성 및 인코딩하여, 상기 인코딩된 상기 제9 큐빗 집합을 상기 제4 통신 주체에게 전송할 수 있다.

[0153] 상기 제4 통신 주체는 제10 큐빗 집합, 제11 큐빗 집합 및 제12 큐빗 집합을 생성 및 인코딩하여, 상기 제1 통신 주체, 상기 제2 통신 주체 및 상기 제3 통신 주체에게 각각 전송할 수 있다.

[0154] 본 발명의 일 실시예에 있어서, 상기 양자 통신 시스템은 상기 제1 통신 주체, 상기 제2 통신 주체, 상기 제3 통신 주체 및 상기 제4 통신 주체와 통신하는 제5 통신 주체를 더 포함할 수 있다. (N이 5인 경우)

[0155] 상기 제1 통신 주체는 제13 큐빗 집합을 생성 및 인코딩하여, 상기 인코딩된 상기 제13 큐빗 집합을 상기 제5 통신 주체에게 전송하고, 상기 제2 통신 주체는 제14 큐빗 집합을 생성 및 인코딩하여, 상기 인코딩된 상기 제14 큐빗 집합을 상기 제5 통신 주체에게 전송하며, 상기 제3 통신 주체는 제15 큐빗 집합을 생성 및 인코딩하여, 상기 인코딩된 상기 제15 큐빗 집합을 상기 제5 통신 주체에게 전송하고, 상기 제4 통신 주체는 제16 큐빗 집합을 생성 및 인코딩하여, 상기 인코딩된 상기 제16 큐빗 집합을 상기 제5 통신 주체에게 전송할 수 있다.

[0156] 상기 제5 통신 주체는 제17 큐빗 집합, 제18 큐빗 집합, 제19 큐빗 집합 및 제20 큐빗 집합을 생성 및 인코딩하여, 상기 제1 통신 주체, 상기 제2 통신 주체, 상기 제3 통신 주체 및 상기 제4 통신 주체에게 각각 전송할 수 있다.

[0157] 본 실시예에 따르면, 양자 통신 방식에 내재되어 있는 공정성을 이용하여 별도의 중재 통신 주체 없이도 복수의 통신 주체들 간에 공정하게 순위를 정할 수 있다.

[0158] 또한, 상기 양자 통신 시스템 내에서 각 통신 주체들이 서로 원거리에 있는 경우라도 복수의 통신 주체들 간에 공정하게 순위를 정할 수 있다.

[0159] 또한, 상기 통신 주체들의 순위는 공정성이 보장되기 때문에 상기 공정한 순위를 기초로 상기 통신 주체들 간에 자원을 공정하게 분배할 수 있다.

[0160] 본 발명의 실시예들에 따른 양자 추첨 방법 및/또는 양자 통신 방법은 임의의 모바일 기기 또는 임의의 컴퓨팅 시스템에 적용될 수 있으며, 본 발명의 실시예들에 따른 양자 통신 시스템에 포함되는 통신 주체는 임의의 모바일 기기 또는 임의의 컴퓨팅 시스템일 수 있다. 예를 들어, 상기 모바일 기기는 휴대폰(Mobile Phone), 스마트 폰(Smart Phone), 태블릿(Tablet) PC(Personal Computer), 노트북(Laptop Computer), 개인 정보 단말기(Personal Digital Assistant; PDA), 휴대형 멀티미디어 플레이어(Portable Multimedia Player; PMP), 디지털 카메라(Digital Camera), 음악 재생기(Music Player), 휴대용 게임 콘솔(Portable Game Console), 네비게이션(Navigation) 시스템 등을 포함할 수 있으며, 웨어러블(wearable) 기기, 사물 인터넷(Internet of Things: IoT) 기기, 만물 인터넷(Internet of Everything: IoE) 기기, e-북(e-book) 등을 더 포함할 수 있다. 상기 컴퓨팅 시스템은 PC(Personal Computer), 서버 컴퓨터(Server Computer), 워크스테이션(Workstation), 디지털 TV(Digital Television), 셋-탑 박스(Set-Top Box) 등을 포함할 수 있다.

[0161] 본 발명의 실시예들에 따른 양자 추첨 방법, 양자 통신 방법 및/또는 양자 통신 시스템은 컴퓨터로 판독 가능한 매체에 저장된 컴퓨터로 판독 가능한 프로그램 코드를 포함하는 제품 등의 형태로 구현될 수 있다. 상기 컴퓨터로 판독 가능한 프로그램 코드는 판독 장치를 통해 다양한 컴퓨터 또는 다른 데이터 처리 장치의 프로세서로 제공될 수 있다. 컴퓨터로 판독 가능한 매체는 컴퓨터로 판독 가능한 신호 매체 또는 컴퓨터로 판독 가능한 기록 매체일 수 있다. 컴퓨터로 판독 가능한 기록 매체는 명령어 실행 시스템, 장비 또는 장치 내에 또는 이들과 접속되어 프로그램을 저장하거나 포함할 수 있는 임의의 유형적인 매체일 수 있다.

산업상 이용가능성

[0162] 본 발명은 다양한 통신 장치 및 통신 시스템에 적용될 수 있다. 따라서 본 발명은 휴대폰, 스마트 폰, PDA, PMP, 디지털 카메라, 캠코더, PC, 서버 컴퓨터, 워크스테이션, 노트북, 디지털 TV, 셋-탑 박스, 음악 재생기, 휴대용 게임 콘솔, 네비게이션 시스템, 스마트 카드, 프린터 등과 같은 다양한 전자 기기에 유용하게 이용될 수 있다.

[0163] 상기에서는 본 발명의 바람직한 실시예를 참조하여 설명하였지만, 해당 기술분야의 숙련된 통상의 기술자는 하기의 특허청구범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 것이다.

부호의 설명

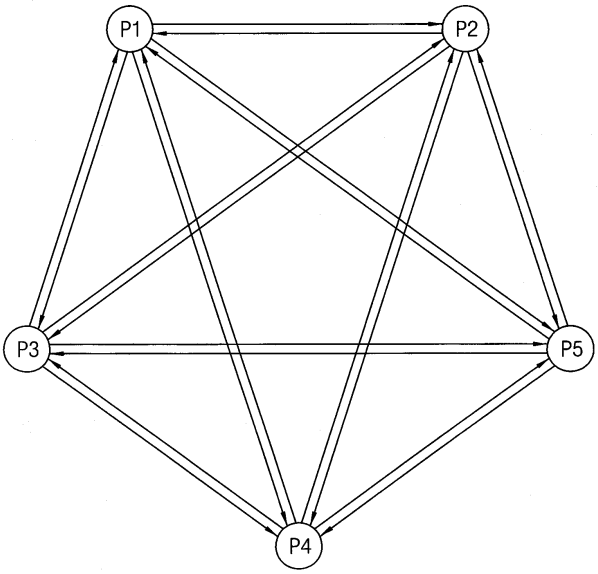
[0164] P1: 제1 통신 주체 P2: 제2 통신 주체

P3: 제3 통신 주체 P4: 제4 통신 주체

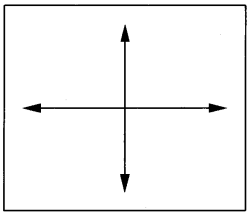
P5: 제5 통신 주체

도면

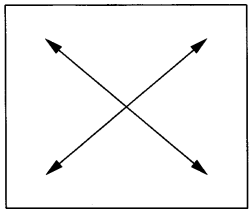
도면1



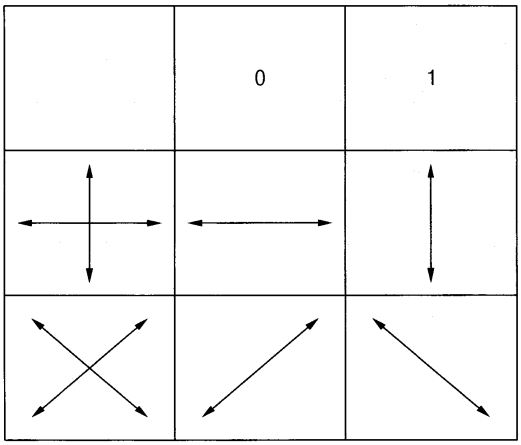
도면2a



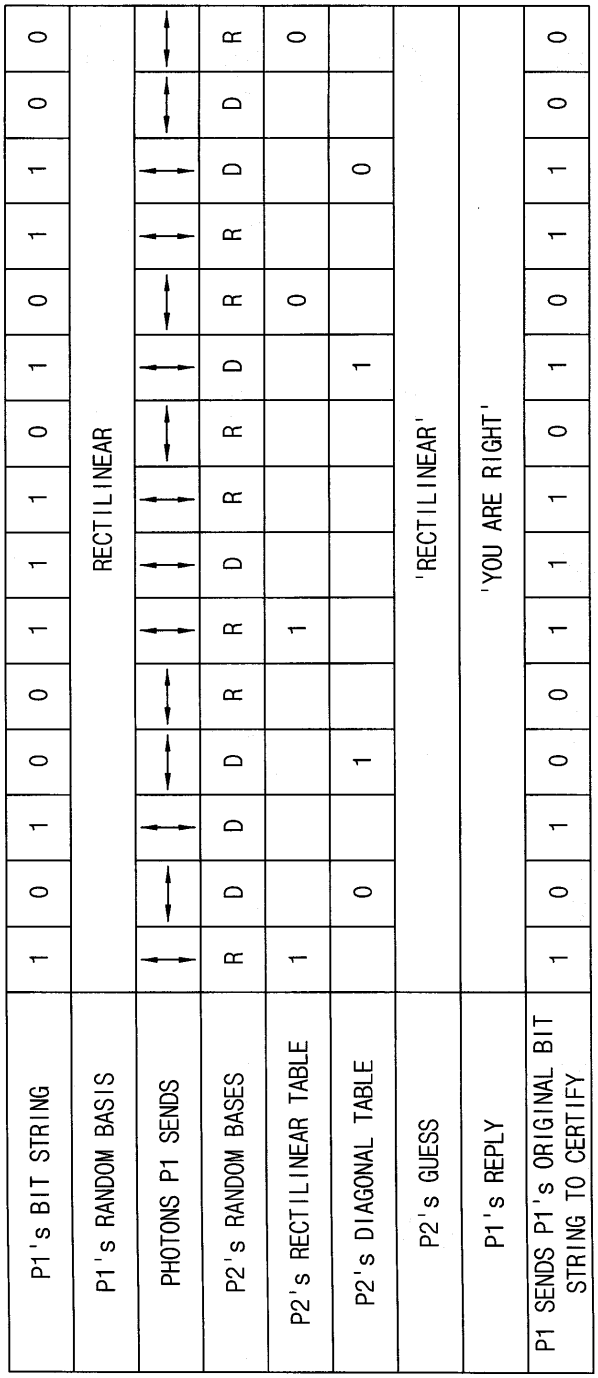
도면2b



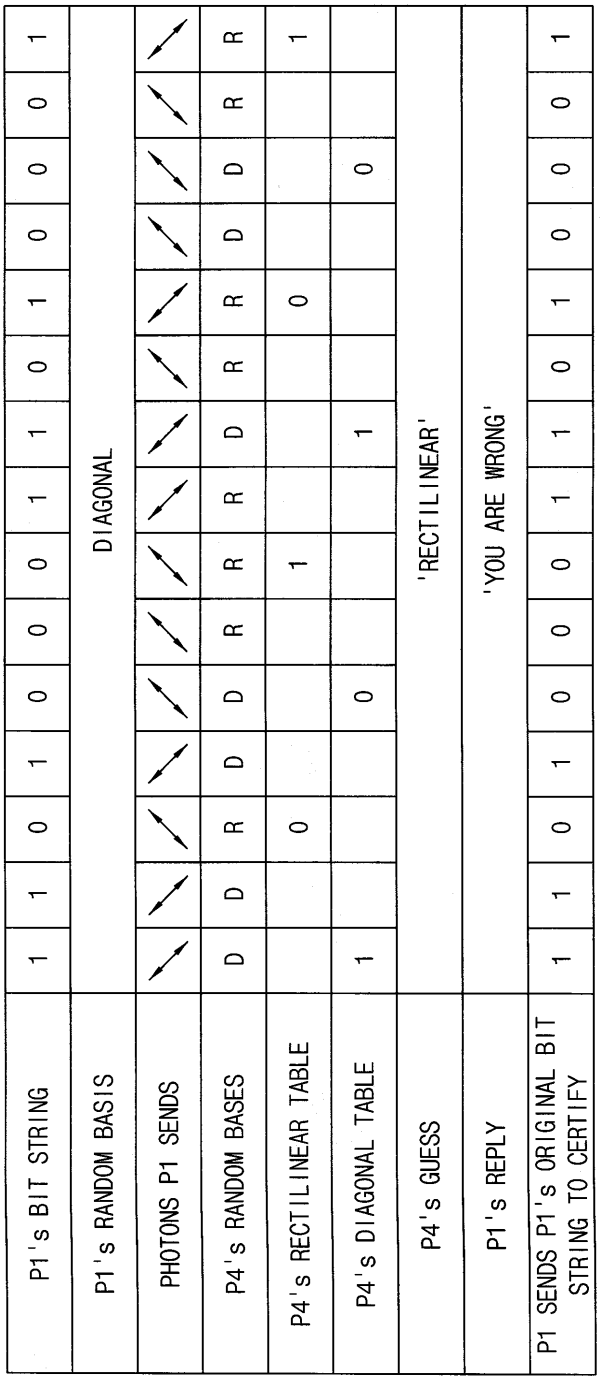
도면3



도면4


P1's BIT STRING
1 0 1 0 0 1 1 1 0 1 0 1 1 0 0
P1's RANDOM BASIS
RECTILINEAR
PHOTONS P1 SENDS
R D D D R R D R R D R R D D R
P2's RANDOM BASES
P2's RECTILINEAR TABLE
1 1 0 0
P2's DIAGONAL TABLE
0 1 1 0
P2's GUESS
'RECTILINEAR'
P1's REPLY
'YOU ARE RIGHT'
P1 SENDS P1's ORIGINAL BIT STRING TO CERTIFY
1 0 1 0 0 1 1 1 0 1 0 1 1 0 0

도면5



P1's BIT STRING	1	1	0	1	0	0	1	1	0	1	0	0	0	1
P1's RANDOM BASIS	DIAGONAL													
PHOTONS P1 SENDS	↘	↘	↗	↗	↗	↗	↘	↘	↗	↘	↗	↗	↗	↘
P4's RANDOM BASES	D	D	R	D	D	R	R	D	R	R	D	D	R	R
P4's RECTILINEAR TABLE			0				1			0				1
P4's DIAGONAL TABLE	1				0			1				0		
P4's GUESS	'RECTILINEAR'													
P1's REPLY	'YOU ARE WRONG'													
P1 SENDS P1's ORIGINAL BIT STRING TO CERTIFY	1	1	0	1	0	0	0	1	1	0	1	0	0	1

도면6a

P1's ANNOUNCEMENT

P2	P3	P4	P5
RIGHT	RIGHT	WRONG	WRONG

도면6b

P2's ANNOUNCEMENT

P1	P3	P4	P5
RIGHT	RIGHT	WRONG	WRONG

도면6c

P3's ANNOUNCEMENT

P1	P2	P4	P5
RIGHT	RIGHT	WRONG	WRONG

도면6d

P4's ANNOUNCEMENT

P1	P2	P3	P5
RIGHT	WRONG	WRONG	WRONG

도면6e

P5's ANNOUNCEMENT

P1	P2	P3	P4
RIGHT	RIGHT	RIGHT	RIGHT

도면7

SORTED LIST

PLAYERS	SCORES	POSITION
P1	4	1
P2	3	2
P3	3	2
P4	1	4
P5	0	5

도면8

UPDATED LIST

PLAYERS	SCORES	POSITION
P1	-	1
P2	0	3
P3	1	2
P4	-	4
P5	-	5