



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2017-0125659
(43) 공개일자 2017년11월15일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) H04L 9/06 (2006.01)
H04L 9/32 (2006.01)
(52) CPC특허분류
H04L 9/0852 (2013.01)
H04L 9/0656 (2013.01)
(21) 출원번호 10-2016-0055781
(22) 출원일자 2016년05월04일
심사청구일자 2016년05월04일

(71) 출원인
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)
(뒷면에 계속)
(74) 대리인
최영한, 지덕규

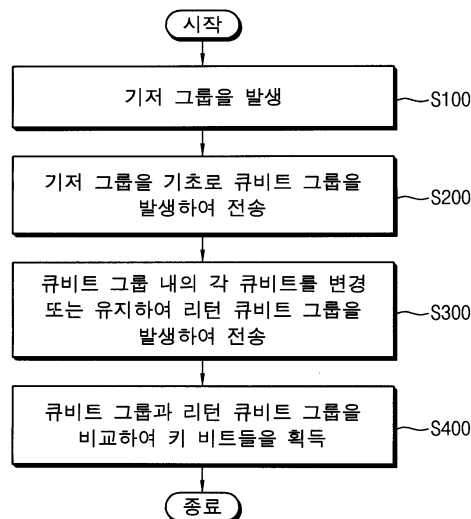
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 양자 통신에서의 다자간 키 분배 방법, 이를 이용하는 양자 통신 방법 및 이를 수행하는 양자 통신 시스템

(57) 요약

양자 통신에서의 다자간 키 분배 방법에서, 제1 및 제2 기저들의 조합으로 이루어지는 복수의 기저 그룹들을 발생한다. 복수의 기저 그룹들을 기초로, 복수의 큐비트들을 각각 포함하는 복수의 큐비트 그룹들을 발생하여 서버에 전송한다. 제1 및 제2 게이트들을 기초로, 복수의 큐비트 그룹들에 포함되는 복수의 큐비트들 각각을 변경 또는 유지하여 복수의 리턴 큐비트 그룹들을 발생하고, 복수의 리턴 큐비트 그룹들을 복수의 사용자 단말기들에 전송한다. 복수의 큐비트 그룹들과 복수의 리턴 큐비트 그룹들을 비교하여, 보안 키를 생성하기 위한 복수의 키 비트들을 획득한다.

대표도 - 도2



(52) CPC특허분류

H04L 9/0819 (2013.01)

H04L 9/3215 (2013.01)

(72) 발명자

정영민

경기도 수원시 영통구 매영로415번길 50 , 스타빌
305호(영통동)

주나이드

경기도 용인시 기흥구 덕영대로 1732, 경희대학교
국제캠퍼스 전자정보관 559호(서천동)

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

명세서

청구범위

청구항 1

복수의 사용자 단말기들이, 제1 기저(basis) 및 제2 기저의 조합으로 이루어지는 복수의 기저 그룹들을 발생하는 단계;

상기 복수의 사용자 단말기들이, 상기 복수의 기저 그룹들을 기초로, 복수의 큐비트(qubit)들을 각각 포함하는 복수의 큐비트 그룹들을 발생하여 서버에 전송하는 단계;

상기 서버가, 제1 게이트 및 제2 게이트를 기초로, 상기 복수의 큐비트 그룹들에 포함되는 상기 복수의 큐비트들 각각을 변경 또는 유지하여 복수의 리턴 큐비트 그룹들을 발생하고, 상기 복수의 리턴 큐비트 그룹들을 상기 복수의 사용자 단말기들에 전송하는 단계; 및

상기 복수의 사용자 단말기들이, 상기 복수의 큐비트 그룹들과 상기 복수의 리턴 큐비트 그룹들을 비교하여, 보안 키를 생성하기 위한 복수의 키(key) 비트들을 획득하는 단계를 포함하는 양자 통신에서의 다자간 키 분배 방법.

청구항 2

제 1 항에 있어서, 상기 복수의 사용자 단말기들 중 제1 사용자 단말기는,

상기 제1 기저 및 상기 제2 기저의 조합으로 이루어지는 제1 기저 그룹을 발생하고,

상기 제1 기저 그룹을 기초로 제1 내지 제N(N은 2 이상의 자연수) 큐비트들을 포함하는 제1 큐비트 그룹을 발생하여 상기 서버에 전송하며,

상기 제1 큐비트 그룹과 상기 서버로부터 전송된 제1 리턴 큐비트 그룹을 비교하여, 상기 복수의 키 비트들을 획득하는 것을 특징으로 하는 양자 통신에서의 다자간 키 분배 방법.

청구항 3

제 2 항에 있어서, 상기 서버는,

상기 제1 내지 제N 큐비트들 각각에 상기 제1 게이트 및 상기 제2 게이트 중 하나를 적용하여, 상기 제1 리턴 큐비트 그룹에 포함되는 제1 내지 제N 리턴 큐비트들 각각을 발생하며,

상기 제1 게이트 및 상기 제2 게이트의 적용 순서에 기초하여 상기 복수의 키 비트들의 값을 결정하는 것을 특징으로 하는 양자 통신에서의 다자간 키 분배 방법.

청구항 4

제 3 항에 있어서, 상기 서버는,

상기 복수의 키 비트들 중 제1 키 비트를 제1 비트 값으로 설정하고자 하는 경우에, 상기 제1 큐비트에 상기 제1 게이트를 적용하여 상기 제1 리턴 큐비트를 발생하고,

상기 제1 키 비트를 상기 제1 비트 값과 다른 제2 비트 값으로 설정하고자 하는 경우에, 상기 제1 큐비트에 상기 제2 게이트를 적용하여 상기 제1 리턴 큐비트를 발생하는 것을 특징으로 하는 양자 통신에서의 다자간 키 분배 방법.

청구항 5

제 4 항에 있어서,

상기 제1 큐비트가 상기 제1 기저에 기초하여 발생된 경우에, 상기 제1 큐비트에 상기 제1 게이트를 적용하여 발생된 상기 제1 리턴 큐비트와 상기 제1 큐비트는 서로 다른 값을 가지고,

상기 제1 큐비트가 상기 제2 기저에 기초하여 발생된 경우에, 상기 제1 큐비트에 상기 제1 게이트를 적용하여 발생된 상기 제1 리턴 큐비트와 상기 제1 큐비트는 동일한 값을 가지는 것을 특징으로 하는 양자 통신에서의 다자간 키 분배 방법.

청구항 6

제 5 항에 있어서,

상기 제1 큐비트가 상기 제1 기저에 기초하여 발생된 경우에, 상기 제1 큐비트에 상기 제2 게이트를 적용하여 발생된 상기 제1 리턴 큐비트와 상기 제1 큐비트는 동일한 값을 가지고,

상기 제1 큐비트가 상기 제2 기저에 기초하여 발생된 경우에, 상기 제1 큐비트에 상기 제2 게이트를 적용하여 발생된 상기 제1 리턴 큐비트와 상기 제1 큐비트는 서로 다른 값을 가지는 것을 특징으로 하는 양자 통신에서의 다자간 키 분배 방법.

청구항 7

제 4 항에 있어서,

상기 제1 기저는 수직 축(vertical axis) 상에서 전자의 스핀 다운(spin down) 또는 스핀 업(spin up)을 나타내기 위한 계산(computational) 기저이고,

상기 제2 기저는 수평 축(horizontal axis) 상에서 상기 전자의 상기 스핀 다운 또는 상기 스핀 업을 나타내기 위한 하다마드(Hadamard) 기저인 것을 특징으로 하는 양자 통신에서의 다자간 키 분배 방법.

청구항 8

제 7 항에 있어서,

상기 제1 게이트는, 상기 제1 큐비트가 상기 계산 기저에 기초하여 발생된 경우에 상기 제1 큐비트의 값을 변경하기 위한 부정 게이트(NOT gate)로서 동작하는 파울리 X 게이트(Pauli X gate)이고,

상기 제2 게이트는, 상기 제1 큐비트가 상기 하다마드 기저에 기초하여 발생된 경우에 상기 제1 큐비트의 값을 변경하기 위한 상기 부정 게이트로서 동작하는 파울리 Z 게이트(Pauli Z gate)인 것을 특징으로 하는 양자 통신에서의 다자간 키 분배 방법.

청구항 9

제 8 항에 있어서,

상기 제1 비트 값은 1이고, 상기 제2 비트 값은 0인 것을 특징으로 하는 양자 통신에서의 다자간 키 분배 방법.

청구항 10

제 1 항에 있어서,

상기 복수의 사용자 단말기들 모두 및 상기 서버는, 동일한 상기 복수의 키 비트들을 공유하는 것을 특징으로 하는 양자 통신에서의 다자간 키 분배 방법.

청구항 11

복수의 사용자 단말기들이, 제1 기저(basis) 및 제2 기저의 조합으로 이루어지는 복수의 기저 그룹들을 발생하는 단계;

상기 복수의 사용자 단말기들이, 상기 복수의 기저 그룹들을 기초로, 복수의 큐비트(qubit)들을 각각 포함하는 복수의 큐비트 그룹들을 발생하여 서버에 전송하는 단계;

상기 서버가, 제1 게이트 및 제2 게이트를 기초로, 상기 복수의 큐비트 그룹들에 포함되는 상기 복수의 큐비트들 각각을 변경 또는 유지하여 복수의 리턴 큐비트 그룹들을 발생하고, 상기 복수의 리턴 큐비트 그룹들을 상기 복수의 사용자 단말기들에 전송하는 단계;

상기 복수의 사용자 단말기들이, 상기 복수의 큐비트 그룹들과 상기 복수의 리턴 큐비트 그룹들을 비교하여, 복

수의 키(key) 비트들을 획득하는 단계;

상기 서버 및 상기 복수의 사용자 단말기들이, 상기 복수의 키 비트들에 대한 정보 조정(information reconciliation) 및 비밀성 증폭(privacy amplification)을 수행하여, 보안 키를 공유하는 단계; 및

상기 서버와 상기 복수의 사용자 단말기들이 상기 보안 키를 기초로 데이터를 암호화하여 교환하는 단계를 포함하는 양자 통신 방법.

청구항 12

제 11 항에 있어서,

상기 복수의 큐비트 그룹들 및 상기 복수의 리턴 큐비트 그룹들은, 상기 서버와 상기 복수의 사용자 단말기들 사이의 양자 채널을 통해 전송되며,

상기 정보 조정 및 상기 비밀성 증폭은, 상기 서버와 상기 복수의 사용자 단말기들 사이의 공개 채널을 통해 수행되는 것을 특징으로 하는 양자 통신 방법.

청구항 13

제 11 항에 있어서,

상기 보안 키의 비트 수는 상기 복수의 키 비트들의 수보다 적은 것을 특징으로 하는 양자 통신 방법.

청구항 14

제 11 항에 있어서,

상기 데이터는 상기 보안 키를 이용하는 원타임 패드(one-time pad) 방식에 의해 암호화되는 것을 특징으로 하는 양자 통신 방법.

청구항 15

제1 기저(basis) 및 제2 기저의 조합으로 이루어지는 복수의 기저 그룹들을 발생하고, 상기 복수의 기저 그룹들을 기초로, 복수의 큐비트(qubit)들을 각각 포함하는 복수의 큐비트 그룹들을 발생하는 복수의 사용자 단말기들; 및

상기 복수의 큐비트 그룹들을 수신하고, 제1 게이트 및 제2 게이트를 기초로, 상기 복수의 큐비트 그룹들에 포함되는 상기 복수의 큐비트들 각각을 변경 또는 유지하여 복수의 리턴 큐비트 그룹들을 발생하며, 상기 복수의 리턴 큐비트 그룹들을 상기 복수의 사용자 단말기들에 전송하는 서버를 포함하고,

상기 복수의 사용자 단말기들은, 상기 복수의 큐비트 그룹들과 상기 복수의 리턴 큐비트 그룹들을 비교하여, 보안 키를 생성하기 위한 복수의 키(key) 비트들을 획득하는 양자 통신 시스템.

청구항 16

제 15 항에 있어서,

상기 복수의 사용자 단말기들 중 제1 사용자 단말기는, 상기 제1 기저 및 상기 제2 기저의 조합으로 이루어지는 제1 기저 그룹을 발생하고, 상기 제1 기저 그룹을 기초로 제1 내지 제N(N은 2 이상의 자연수) 큐비트들을 포함하는 제1 큐비트 그룹을 발생하여 상기 서버에 전송하고, 상기 제1 큐비트 그룹과 상기 서버로부터 전송된 제1 리턴 큐비트 그룹을 비교하여, 상기 복수의 키 비트들을 획득하며,

상기 서버는, 상기 제1 내지 제N 큐비트들 각각에 상기 제1 게이트 및 상기 제2 게이트 중 하나를 적용하여, 상기 제1 리턴 큐비트 그룹에 포함되는 제1 내지 제N 리턴 큐비트들 각각을 발생하고, 상기 제1 게이트 및 상기 제2 게이트의 적용 순서에 기초하여 상기 복수의 키 비트들의 값을 결정하는 것을 특징으로 하는 양자 통신 시스템.

청구항 17

제 16 항에 있어서, 상기 서버는,

상기 복수의 키 비트들 중 제1 키 비트를 제1 비트 값으로 설정하고자 하는 경우에, 상기 제1 큐비트에 상기 제1 게이트를 적용하여 상기 제1 리턴 큐비트를 발생하고,

상기 제1 키 비트를 상기 제1 비트 값과 다른 제2 비트 값으로 설정하고자 하는 경우에, 상기 제1 큐비트에 상기 제2 게이트를 적용하여 상기 제1 리턴 큐비트를 발생하는 것을 특징으로 하는 양자 통신 시스템.

청구항 18

제 17 항에 있어서,

상기 제1 큐비트가 상기 제1 기저에 기초하여 발생된 경우에, 상기 제1 큐비트에 상기 제1 게이트를 적용하여 발생된 상기 제1 리턴 큐비트와 상기 제1 큐비트는 서로 다른 값을 가지고,

상기 제1 큐비트가 상기 제2 기저에 기초하여 발생된 경우에, 상기 제1 큐비트에 상기 제1 게이트를 적용하여 발생된 상기 제1 리턴 큐비트와 상기 제1 큐비트는 동일한 값을 가지는 것을 특징으로 하는 양자 통신 시스템.

청구항 19

제 18 항에 있어서,

상기 제1 큐비트가 상기 제1 기저에 기초하여 발생된 경우에, 상기 제1 큐비트에 상기 제2 게이트를 적용하여 발생된 상기 제1 리턴 큐비트와 상기 제1 큐비트는 동일한 값을 가지고,

상기 제1 큐비트가 상기 제2 기저에 기초하여 발생된 경우에, 상기 제1 큐비트에 상기 제2 게이트를 적용하여 발생된 상기 제1 리턴 큐비트와 상기 제1 큐비트는 서로 다른 값을 가지는 것을 특징으로 하는 양자 통신 시스템.

청구항 20

제 15 항에 있어서,

상기 서버 및 상기 복수의 사용자 단말기들은, 상기 복수의 키 비트들에 대한 정보 조정(information reconciliation) 및 비밀성 증폭(privacy amplification)을 수행하여, 상기 보안 키를 공유하며,

상기 서버와 상기 복수의 사용자 단말기들이 상기 보안 키를 기초로 데이터를 암호화하여 교환하는 것을 특징으로 하는 양자 통신 시스템.

발명의 설명

기술 분야

[0001] 본 발명은 통신 시스템에 관한 것으로서, 더욱 상세하게는 양자 통신에서의 다자간 키 분배 방법, 상기 다자간 키 분배 방법을 이용하는 양자 통신 방법, 상기 다자간 키 분배 방법 및/또는 상기 양자 통신 방법을 수행하는 양자 통신 시스템에 관한 것이다.

배경 기술

[0002] 1984년 C. H. Bennett과 G. Brassard에 의해 고안된 양자 키 분배(quantum key distribution: QKD) 프로토콜은 BB84 프로토콜로 불릴 수 있다. 상기과 같은 BB84 프로토콜이 알려진 이후 양자 암호 분야에 엄청난 발전이 있어 왔다. 양자 키 분배 프로토콜의 핵심은 멀리 떨어져 있는 두 사용자가 공개된 통신 채널을 통해 암호 통신을 위한 비밀 키를 생성 및 공유하며, 동시에 공유된 비밀 키에 대한 무조건적 안전성(unconditional security)을 보장한다는 점이다.

[0003] 일반적으로, 상기과 같은 양자 키 분배 프로토콜은 두 사용자가 키를 공유하는 경우에 기초하여 연구되고 있으나, 복수의 사용자들이 키를 공유하는 경우에 대한 연구도 필요하다.

발명의 내용

해결하려는 과제

[0004] 본 발명의 일 목적은 복수의 사용자 단말기들이 효율적으로 키를 공유할 수 있는 양자 통신에서의 다자간 키 분

배 방법을 제공하는 것이다.

[0005] 본 발명의 다른 목적은 상기 다자간 키 분배 방법을 이용하는 양자 통신 방법을 제공하는 것이다.

[0006] 본 발명의 또 다른 목적은 상기 다자간 키 분배 방법 및/또는 상기 양자 통신 방법을 수행하는 양자 통신 시스템을 제공하는 것이다.

과제의 해결 수단

[0007] 상기 일 목적을 달성하기 위해, 본 발명의 실시예들에 따른 양자 통신에서의 다자간 키 분배 방법에서, 복수의 사용자 단말기들이, 제1 기저(basis) 및 제2 기저의 조합으로 이루어지는 복수의 기저 그룹들을 발생한다. 상기 복수의 사용자 단말기들이, 상기 복수의 기저 그룹들을 기초로, 복수의 큐비트(qubit)들을 각각 포함하는 복수의 큐비트 그룹들을 발생하여 서버에 전송한다. 상기 서버가, 제1 게이트 및 제2 게이트를 기초로, 상기 복수의 큐비트 그룹들에 포함되는 상기 복수의 큐비트들 각각을 변경 또는 유지하여 복수의 리턴 큐비트 그룹들을 발생하고, 상기 복수의 리턴 큐비트 그룹들을 상기 복수의 사용자 단말기들에 전송한다. 상기 복수의 사용자 단말기들이, 상기 복수의 큐비트 그룹들과 상기 복수의 리턴 큐비트 그룹들을 비교하여, 보안 키를 생성하기 위한 복수의 키(key) 비트들을 획득한다.

[0008] 일 실시예에서, 상기 복수의 사용자 단말기들 중 제1 사용자 단말기는, 상기 제1 기저 및 상기 제2 기저의 조합으로 이루어지는 제1 기저 그룹을 발생하고, 상기 제1 기저 그룹을 기초로 제1 내지 제N(N은 2 이상의 자연수) 큐비트들을 포함하는 제1 큐비트 그룹을 발생하여 상기 서버에 전송하며, 상기 제1 큐비트 그룹과 상기 서버로부터 전송된 제1 리턴 큐비트 그룹을 비교하여, 상기 복수의 키 비트들을 획득할 수 있다.

[0009] 일 실시예에서, 상기 서버는, 상기 제1 내지 제N 큐비트들 각각에 상기 제1 게이트 및 상기 제2 게이트 중 하나를 적용하여, 상기 제1 리턴 큐비트 그룹에 포함되는 제1 내지 제N 리턴 큐비트들 각각을 발생하며, 상기 제1 게이트 및 상기 제2 게이트의 적용 순서에 기초하여 상기 복수의 키 비트들의 값을 결정할 수 있다.

[0010] 일 실시예에서, 상기 서버는, 상기 복수의 키 비트들 중 제1 키 비트를 제1 비트 값으로 설정하고자 하는 경우에, 상기 제1 큐비트에 상기 제1 게이트를 적용하여 상기 제1 리턴 큐비트를 발생하고, 상기 제1 키 비트를 상기 제1 비트 값과 다른 제2 비트 값으로 설정하고자 하는 경우에, 상기 제1 큐비트에 상기 제2 게이트를 적용하여 상기 제1 리턴 큐비트를 발생할 수 있다.

[0011] 일 실시예에서, 상기 제1 큐비트가 상기 제1 기저에 기초하여 발생된 경우에, 상기 제1 큐비트에 상기 제1 게이트를 적용하여 발생된 상기 제1 리턴 큐비트와 상기 제1 큐비트는 서로 다른 값을 가질 수 있다. 상기 제1 큐비트가 상기 제2 기저에 기초하여 발생된 경우에, 상기 제1 큐비트에 상기 제1 게이트를 적용하여 발생된 상기 제1 리턴 큐비트와 상기 제1 큐비트는 동일한 값을 가질 수 있다.

[0012] 일 실시예에서, 상기 제1 큐비트가 상기 제1 기저에 기초하여 발생된 경우에, 상기 제1 큐비트에 상기 제2 게이트를 적용하여 발생된 상기 제1 리턴 큐비트와 상기 제1 큐비트는 동일한 값을 가질 수 있다. 상기 제1 큐비트가 상기 제2 기저에 기초하여 발생된 경우에, 상기 제1 큐비트에 상기 제2 게이트를 적용하여 발생된 상기 제1 리턴 큐비트와 상기 제1 큐비트는 서로 다른 값을 가질 수 있다.

[0013] 일 실시예에서, 상기 제1 기저는 수직 축(vertical axis) 상에서 전자의 스핀 다운(spin down) 또는 스핀 업(spin up)을 나타내기 위한 계산(computational) 기저일 수 있다. 상기 제2 기저는 수평 축(horizontal axis) 상에서 상기 전자의 상기 스핀 다운 또는 상기 스핀 업을 나타내기 위한 하다마드(Hadamard) 기저일 수 있다.

[0014] 일 실시예에서, 상기 제1 게이트는, 상기 제1 큐비트가 상기 계산 기저에 기초하여 발생된 경우에 상기 제1 큐비트의 값을 변경하기 위한 부정 게이트(NOT gate)로서 동작하는 파울리 X 게이트(Pauli X gate)일 수 있다. 상기 제2 게이트는, 상기 제1 큐비트가 상기 하다마드 기저에 기초하여 발생된 경우에 상기 제1 큐비트의 값을 변경하기 위한 상기 부정 게이트로서 동작하는 파울리 Z 게이트(Pauli Z gate)일 수 있다.

[0015] 일 실시예에서, 상기 제1 비트 값은 1이고, 상기 제2 비트 값은 0일 수 있다.

[0016] 일 실시예에서, 상기 복수의 사용자 단말기들 모두 및 상기 서버는, 동일한 상기 복수의 키 비트들을 공유할 수 있다.

[0017] 상기 다른 목적을 달성하기 위해, 본 발명의 실시예들에 따른 양자 통신 방법에서, 복수의 사용자 단말기들이, 제1 기저(basis) 및 제2 기저의 조합으로 이루어지는 복수의 기저 그룹들을 발생한다. 상기 복수의 사용자 단말기들이, 상기 복수의 기저 그룹들을 기초로, 복수의 큐비트(qubit)들을 각각 포함하는 복수의 큐비트 그룹들을

발생하여 서버에 전송한다. 상기 서버가, 제1 게이트 및 제2 게이트를 기초로, 상기 복수의 큐비트 그룹들에 포함되는 상기 복수의 큐비트들 각각을 변경 또는 유지하여 복수의 리턴 큐비트 그룹들을 발생하고, 상기 복수의 리턴 큐비트 그룹들을 상기 복수의 사용자 단말기들에 전송한다. 상기 복수의 사용자 단말기들이, 상기 복수의 큐비트 그룹들과 상기 복수의 리턴 큐비트 그룹들을 비교하여, 복수의 키(key) 비트들을 획득한다. 상기 서버 및 상기 복수의 사용자 단말기들이, 상기 복수의 키 비트들에 대한 정보 조정(information reconciliation) 및 비밀성 증폭(privacy amplification)을 수행하여, 보안 키를 공유한다. 상기 서버와 상기 복수의 사용자 단말기들이 상기 보안 키를 기초로 데이터를 암호화하여 교환한다.

[0018] 일 실시예에서, 상기 복수의 큐비트 그룹들 및 상기 복수의 리턴 큐비트 그룹들은, 상기 서버와 상기 복수의 사용자 단말기들 사이의 양자 채널을 통해 전송될 수 있다. 상기 정보 조정 및 상기 비밀성 증폭은, 상기 서버와 상기 복수의 사용자 단말기들 사이의 공개 채널을 통해 수행될 수 있다.

[0019] 일 실시예에서, 상기 보안 키의 비트 수는 상기 복수의 키 비트들의 수보다 적을 수 있다.

[0020] 일 실시예에서, 상기 데이터는 상기 보안 키를 이용하는 원타임 패드(one-time pad) 방식에 의해 암호화될 수 있다.

[0021] 상기 또 다른 목적을 달성하기 위해, 본 발명의 실시예들에 따른 양자 통신 시스템은 복수의 사용자 단말기들 및 서버를 포함한다. 상기 복수의 사용자 단말기들은 제1 기저(basis) 및 제2 기저의 조합으로 이루어지는 복수의 기저 그룹들을 발생하고, 상기 복수의 기저 그룹들을 기초로, 복수의 큐비트(qubit)들을 각각 포함하는 복수의 큐비트 그룹들을 발생한다. 상기 서버는 상기 복수의 큐비트 그룹들을 수신하고, 제1 게이트 및 제2 게이트를 기초로, 상기 복수의 큐비트 그룹들에 포함되는 상기 복수의 큐비트들 각각을 변경 또는 유지하여 복수의 리턴 큐비트 그룹들을 발생하며, 상기 복수의 리턴 큐비트 그룹들을 상기 복수의 사용자 단말기들에 전송한다. 상기 복수의 사용자 단말기들은, 상기 복수의 큐비트 그룹들과 상기 복수의 리턴 큐비트 그룹들을 비교하여, 보안 키를 생성하기 위한 복수의 키(key) 비트들을 획득한다.

[0022] 일 실시예에서, 상기 복수의 사용자 단말기들 중 제1 사용자 단말기는, 상기 제1 기저 및 상기 제2 기저의 조합으로 이루어지는 제1 기저 그룹을 발생하고, 상기 제1 기저 그룹을 기초로 제1 내지 제N(N은 2 이상의 자연수) 큐비트들을 포함하는 제1 큐비트 그룹을 발생하여 상기 서버에 전송하고, 상기 제1 큐비트 그룹과 상기 서버로부터 전송된 제1 리턴 큐비트 그룹을 비교하여, 상기 복수의 키 비트들을 획득할 수 있다. 상기 서버는, 상기 제1 내지 제N 큐비트들 각각에 상기 제1 게이트 및 상기 제2 게이트 중 하나를 적용하여, 상기 제1 리턴 큐비트 그룹에 포함되는 제1 내지 제N 리턴 큐비트들 각각을 발생하고, 상기 제1 게이트 및 상기 제2 게이트의 적용 순서에 기초하여 상기 복수의 키 비트들의 값을 결정할 수 있다.

[0023] 일 실시예에서, 상기 서버는, 상기 복수의 키 비트들 중 제1 키 비트를 제1 비트 값으로 설정하고자 하는 경우에, 상기 제1 큐비트에 상기 제1 게이트를 적용하여 상기 제1 리턴 큐비트를 발생하고, 상기 제1 키 비트를 상기 제1 비트 값과 다른 제2 비트 값으로 설정하고자 하는 경우에, 상기 제1 큐비트에 상기 제2 게이트를 적용하여 상기 제1 리턴 큐비트를 발생할 수 있다.

[0024] 일 실시예에서, 상기 제1 큐비트가 상기 제1 기저에 기초하여 발생된 경우에, 상기 제1 큐비트에 상기 제1 게이트를 적용하여 발생된 상기 제1 리턴 큐비트와 상기 제1 큐비트는 서로 다른 값을 가질 수 있다. 상기 제1 큐비트가 상기 제2 기저에 기초하여 발생된 경우에, 상기 제1 큐비트에 상기 제1 게이트를 적용하여 발생된 상기 제1 리턴 큐비트와 상기 제1 큐비트는 동일한 값을 가질 수 있다.

[0025] 일 실시예에서, 상기 제1 큐비트가 상기 제1 기저에 기초하여 발생된 경우에, 상기 제1 큐비트에 상기 제2 게이트를 적용하여 발생된 상기 제1 리턴 큐비트와 상기 제1 큐비트는 동일한 값을 가질 수 있다. 상기 제1 큐비트가 상기 제2 기저에 기초하여 발생된 경우에, 상기 제1 큐비트에 상기 제2 게이트를 적용하여 발생된 상기 제1 리턴 큐비트와 상기 제1 큐비트는 서로 다른 값을 가질 수 있다.

[0026] 일 실시예에서, 상기 서버 및 상기 복수의 사용자 단말기들은, 상기 복수의 키 비트들에 대한 정보 조정(information reconciliation) 및 비밀성 증폭(privacy amplification)을 수행하여, 상기 보안 키를 공유할 수 있다. 상기 서버와 상기 복수의 사용자 단말기들이 상기 보안 키를 기초로 데이터를 암호화하여 교환할 수 있다.

발명의 효과

[0027] 상기과 같은 본 발명의 실시예들에 따른 양자 통신에서의 다자간 키 교환 방법 및 양자 통신 방법에서는, 사용

자 단말기들이 서버와의 통신을 통해 키 비트들을 공유할 수 있다. 이 때, 서버는 큐비트들을 직접 발생하지 않고, 사용자 단말기들에서 발생된 큐비트들에 제1 및 제2 게이트들을 선택적으로 적용한 후에 큐비트들을 사용자 단말기들에 되돌려줌으로써, 상기 키 비트들과 관련된 정보를 사용자 단말기들에 전송할 수 있다. 따라서, 키 비트 전송을 위한 서버의 부하가 감소될 수 있으며, 복수의 사용자 단말기들이 동일한 키 비트들을 효율적으로 공유할 수 있다. 또한, 양자 통신에서의 다자간 키 교환 방법 및/또는 양자 통신 방법을 수행하는 양자 통신 시스템의 성능이 향상될 수 있다.

도면의 간단한 설명

도 1은 본 발명의 실시예들에 따른 양자 통신 시스템을 나타내는 블록도이다.

도 2는 본 발명의 실시예들에 따른 양자 통신에서의 다자간 키 분배 방법을 나타내는 순서도이다.

도 3은 도 1의 양자 통신 시스템에 포함되는 서버 및 제1 사용자 단말기의 일 예를 나타내는 블록도이다.

도 4, 5a, 5b, 6 및 7은 본 발명의 실시예들에 따른 양자 통신에서의 다자간 키 분배 방법을 설명하기 위한 표들이다.

도 8은 본 발명의 실시예들에 따른 양자 통신 방법을 나타내는 순서도이다.

발명을 실시하기 위한 구체적인 내용

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.

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.

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.

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.

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 실시된 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.

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.

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.

이하, 첨부한 도면들을 참조하여, 본 발명의 바람직한 실시예를 보다 상세하게 설명하고자 한다. 도면상의 동일

한 구성요소에 대해서는 동일한 참조부호를 사용하고 동일한 구성요소에 대해서 중복된 설명은 생략한다.

- [0037] 도 1은 본 발명의 실시예들에 따른 양자 통신 시스템을 나타내는 블록도이다.
- [0038] 도 1을 참조하면, 양자 통신 시스템(10)은 서버(100) 및 복수의 사용자 단말기들(200, 300, 400, 500)을 포함한다.
- [0039] 양자 통신 시스템(10)은 양자역학(quantum mechanics)을 이용하여 구현되는 통신 방식이며, 전자(electron)의 회전 상태(spin)에 기초하여 정보를 전달할 수 있다.
- [0040] 본 발명의 실시예들에 따른 양자 통신 시스템(10)에서, 사용자 단말기들(200, 300, 400, 500)은 서버(100)와의 통신을 통해 동일한 키(key) 비트(bit)들을 공유한다. 서버(100)가 상기 키 비트들을 결정하고, 사용자 단말기들(200, 300, 400, 500)이 상기 결정된 키 비트들을 획득한다. 이 때, 사용자 단말기들(200, 300, 400, 500)이 큐비트(qubit)들을 발생하며, 서버(100)는 큐비트들의 발생 없이 사용자 단말기들(200, 300, 400, 500)에서 발생된 상기 큐비트들에 기초하여 상기 키 비트들과 관련된 정보를 사용자 단말기들(200, 300, 400, 500)에 전송한다.
- [0041] 사용자 단말기들(200, 300, 400, 500) 각각과 서버(100)는 두 개의 채널들을 통해 연결될 수 있다. 상기 두 개의 채널들 중 하나는 상기 큐비트들을 전송하기 위한 양자 채널(quantum channel) 또는 보안 채널(secure channel)일 수 있고, 상기 두 개의 채널들 중 다른 하나는 일반 데이터 비트들을 전송하기 위한 공개 채널(public channel) 또는 고전 채널(classical channel)일 수 있다. 도 1에서, 상기 양자 채널을 실선의 양방향 화살표로 도시하였고, 상기 공개 채널을 점선의 양방향 화살표로 도시하였다.
- [0042] 사용자 단말기들(200, 300, 400, 500) 중 인접한 두 개는 하나의 채널을 통해 연결될 수 있다. 상기 하나의 채널은 상기 공개 채널 또는 상기 고전 채널일 수 있다.
- [0043] 도 1에서는 양자 통신 시스템(10)이 네 개의 사용자 단말기들(200, 300, 400, 500)을 포함하는 것으로 도시하였으나, 실시예에 따라서 양자 통신 시스템(10)은 임의의 M(M은 자연수)개의 사용자 단말기를 포함하여 구현될 수 있다.
- [0044] 도 2는 본 발명의 실시예들에 따른 양자 통신에서의 다자간 키 분배 방법을 나타내는 순서도이다.
- [0045] 도 1 및 2를 참조하면, 본 발명의 실시예들에 따른 양자 통신에서의 다자간 키 분배 방법에서, 복수의 사용자 단말기들(200, 300, 400, 500)은 복수의 기저(basis) 그룹들을 발생한다(단계 S100). 상기 복수의 기저 그룹들 각각은, 제1 기저(basis) 및 상기 제1 기저와 다른 제2 기저의 조합으로 이루어진다. 도 4를 참조하여 후술하는 것처럼, 상기 제1 및 제2 기저들 각각은 큐비트를 발생 또는 판별하는데 이용될 수 있다.
- [0046] 사용자 단말기들(200, 300, 400, 500)은 상기 복수의 기저 그룹들을 기초로 복수의 큐비트 그룹들을 발생하여 서버(100)에 전송한다(단계 S200). 상기 복수의 큐비트 그룹들 각각은 복수의 큐비트들을 포함할 수 있다. 도 4를 참조하여 후술하는 것처럼, 상기 큐비트는 양자 통신에서 이용되는 비트를 나타낼 수 있으며, 상기 제1 및 제2 기저들 중 하나에 기초하여 발생되고 "0" 및 "1" 중 하나에 상응하는 값을 가질 수 있다.
- [0047] 서버(100)는 제1 게이트 및 상기 제1 게이트와 다른 제2 게이트를 기초로, 상기 복수의 큐비트 그룹들에 포함되는 상기 복수의 큐비트들 각각을 변경 또는 유지하여 복수의 리턴 큐비트 그룹들을 발생하고, 상기 복수의 리턴 큐비트 그룹들을 사용자 단말기들(200, 300, 400, 500)에 전송한다(단계 S300).
- [0048] 일 실시예에서, 서버(100)는 각 큐비트 그룹에 포함되는 상기 복수의 큐비트들 각각에 상기 제1 및 제2 게이트들 중 하나를 적용하여, 각 리턴 큐비트 그룹에 포함되는 복수의 리턴 큐비트들 각각을 발생할 수 있다. 하나의 큐비트 그룹 내의 큐비트들의 개수는 하나의 리턴 큐비트 그룹 내의 리턴 큐비트들의 개수와 실질적으로 동일할 수 있다. 하나의 큐비트 그룹 내의 하나의 큐비트와 이에 상응하는 하나의 리턴 큐비트 그룹 내의 하나의 리턴 큐비트는, 큐비트의 발생 시에 사용된 기저의 종류 및 리턴 큐비트의 발생 시에 적용된 게이트의 종류에 따라, 동일한 값을 가지거나 서로 다른 값을 가질 수 있다.
- [0049] 일 실시예에서, 서버(100)는 상기 제1 및 제2 게이트들의 적용 순서에 기초하여 상기 복수의 키 비트들의 값을 결정할 수 있다. 이에 대해서는 도 6 및 7을 참조하여 후술하도록 한다.
- [0050] 사용자 단말기들(200, 300, 400, 500)은 상기 복수의 큐비트 그룹들과 상기 복수의 리턴 큐비트 그룹들을 비교하여, 상기 복수의 키 비트들을 획득한다(단계 S400). 도 8을 참조하여 후술하는 것처럼, 상기 복수의 키 비트들은 양자 통신 시스템(10)에서 보안 통신을 수행하기 위한 보안 키를 생성하는데 이용될 수 있다.

- [0051] 사용자 단말기들(200, 300, 400, 500)이 발생하는 상기 복수의 큐비트 그룹들은 서로 상이할 수 있지만, 서버(100)가 상기 복수의 큐비트 그룹들 모두에 대해 동일한 순서로 상기 제1 및 제2 게이트들을 적용하여 상기 복수의 리턴 큐비트 그룹들을 발생시킬 수 있다. 따라서, 복수의 사용자 단말기들(200, 300, 400, 500) 모두 및 서버(100)는 실질적으로 동일한 상기 복수의 키 비트들을 공유할 수 있다.
- [0052] 한편, 도 2에서 도시하지는 않았지만, 도 8을 참조하여 후술하는 것처럼 단계 S400 이후에, 서버(100)와 사용자 단말기들(200, 300, 400, 500)이 상기 복수의 키 비트들에 대한 정보 조정(information reconciliation) 및 비밀성 증폭(privacy amplification)을 수행하여, 상기 보안 키를 공유할 수 있다. 상기와 같은 다자간 키 분배 동작 이후에, 양자 통신 시스템(10) 내에서 상기 보안 키에 기초하여 데이터를 암호화하여 교환할 수 있다.
- [0053] 본 발명의 실시예들에 따른 양자 통신에서의 다자간 키 분배 방법에서는, 사용자 단말기들(200, 300, 400, 500)이 서버(100)와의 통신을 통해 상기 키 비트들을 공유할 수 있다. 이 때, 서버(100)는 큐비트들을 직접 발생하지 않고, 사용자 단말기들(200, 300, 400, 500)에서 발생된 큐비트들에 상기 제1 및 제2 게이트들을 선택적으로 적용한 후에 상기 큐비트들을 사용자 단말기들(200, 300, 400, 500)에 되돌려줌으로써, 상기 키 비트들과 관련된 정보를 사용자 단말기들(200, 300, 400, 500)에 전송할 수 있다. 따라서, 서버(100)의 부하(load)가 감소될 수 있으며, 사용자 단말기들(200, 300, 400, 500)이 동일한 키 비트들을 효율적으로 공유할 수 있다.
- [0054] 이하에서는, 서버(100)와 하나의 사용자 단말기(예를 들어, 제1 사용자 단말기(200))에 기초하여, 본 발명의 실시예들에 따른 양자 통신 시스템(10)의 동작(예를 들어, 다자간 키 분배 동작)을 보다 상세하게 설명하도록 한다.
- [0055] 도 3은 도 1의 양자 통신 시스템에 포함되는 서버 및 제1 사용자 단말기의 일 예를 나타내는 블록도이다. 도 4, 5a, 5b, 6 및 7은 본 발명의 실시예들에 따른 양자 통신에서의 다자간 키 분배 방법을 설명하기 위한 표들이다.
- [0056] 도 3 및 6을 참조하면, 서버(100)는 송수신부(110), 랜덤 넘버 발생부(120) 및 리턴 큐비트 발생부(130)를 포함할 수 있다. 제1 사용자 단말기(200)는 랜덤 넘버 발생부(210), 기저 결정부(220), 데이터 제공부(230), 큐비트 발생부(240), 송수신부(250) 및 키 발생부(260)를 포함할 수 있다. 채널들(202, 204)은 서버(100)와 제1 사용자 단말기(200) 사이에 연결되어 정보 전달 경로를 제공할 수 있다.
- [0057] 랜덤 넘버 발생부(210)는 제1 랜덤 넘버(RN1)를 발생할 수 있다. 예를 들어, 제1 랜덤 넘버(RN1)는 N (N 은 자연수)비트의 임의의 이진(binary) 넘버일 수 있다. 랜덤 넘버 발생부(210)는 제1 랜덤 넘버(RN1)를 발생하기 위한 임의의 랜덤 넘버 발생기를 포함할 수도 있고, 사용자 설정 신호에 기초하여 수동으로(manually) 제1 랜덤 넘버(RN1)를 발생할 수도 있다.
- [0058] 기저 결정부(220)는 제1 기저 그룹(BG1)을 발생할 수 있다. 예를 들어, 기저 결정부(220)는 제1 랜덤 넘버(RN1)의 각 비트를 상기 제1 및 제2 기저들 중 하나로 변환하여 제1 기저 그룹(BG1)을 발생할 수 있다. 예를 들어, 제1 랜덤 넘버(RN1)는 K (K 는 0 이상 N 이하의 정수)개의 제1 비트 값(예를 들어, "1")과 상기 제1 비트 값과 다른 ($N-K$)개의 제2 비트 값(예를 들어, "0")의 조합으로 이루어지는 N 비트의 이진 넘버일 수 있다. 이 경우, 기저 결정부(220)는 제1 랜덤 넘버(RN1)의 상기 제1 비트 값을 상기 제1 기저로 변환하고 제1 랜덤 넘버(RN1)의 상기 제2 비트 값을 상기 제2 기저로 변환하여, N 개의 상기 제1 및 제2 기저들의 조합으로 이루어지는 제1 기저 그룹(BG1)을 발생할 수 있다.
- [0059] 도 4를 참조하면, 상기 제1 기저는 수직 축(vertical axis) 상에서 전자의 스핀 다운(spin down) 또는 스핀 업(spin up)을 나타내기 위한 계산(computational) 기저일 수 있고, 상기 제2 기저는 수평 축(horizontal axis) 상에서 상기 전자의 상기 스핀 다운 또는 상기 스핀 업을 나타내기 위한 하다마드(Hadamard) 기저일 수 있다. 상기 계산 기저는 "+"로 표기될 수 있고, 상기 하다마드 기저는 "×"로 표기될 수 있다.
- [0060] 상기 계산 기저에서, 상기 스핀 다운 상태를 가지는 전자는 큐비트($|0\rangle$)로 표기될 수 있고, 상기 스핀 업 상태를 가지는 전자는 큐비트($|1\rangle$)로 표기될 수 있다. 상기 하다마드 기저에서, 상기 스핀 다운 상태를 가지는 전자는 큐비트($|+\rangle$)로 표기될 수 있고, 상기 스핀 업 상태를 가지는 전자는 큐비트($|-\rangle$)로 표기될 수 있다.
- [0061] 일 실시예에서, 상기 계산 기저의 큐비트($|0\rangle$)는 이진 비트의 "0"에 상응할 수 있고, 상기 계산 기저의 큐비트($|1\rangle$)는 상기 이진 비트의 "1"에 상응할 수 있다. 이와 유사하게, 상기 하다마드 기저의 큐비트($|+\rangle$)는 상기 이진 비트의 "0"에 상응할 수 있고, 상기 하다마드 기저의 큐비트($|-\rangle$)는 상기 이진 비트의 "1"에 상응할 수 있다. 다른 실시예에서, 큐비트들($|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$) 각각이 나타내는 상기 이진 비트의 값("0" 또는 "1")은 변경될 수 있다.

- [0062] 다시 도 3 및 6을 참조하면, N이 10인 경우에 기초하여 제1 사용자 단말기(200)의 제1 기저 그룹(BG1)의 발생 동작을 설명할 수 있다. 예를 들어, 랜덤 넘버 발생부(210)는 "1101001001"의 10비트의 제1 랜덤 넘버(RN1)를 발생할 수 있다. 기저 결정부(220)는 "1101001001"의 제1 랜덤 넘버(RN1)에 기초하여 "+ + × + × × + × × +"의 제1 기저 그룹(BG1)을 발생할 수 있다.
- [0063] 데이터 제공부(230)는 제1 데이터(DAT1)를 발생할 수 있다. 예를 들어, 제1 랜덤 넘버(RN1)와 유사하게, 제1 데이터(DAT1)는 N비트의 임의의 이진 데이터일 수 있다. 랜덤 넘버 발생부(210)와 유사하게, 데이터 제공부(230)는 임의의 랜덤 넘버 발생기를 포함하거나, 사용자 설정 신호에 기초하여 제1 데이터(DAT1)를 발생할 수도 있다. 도시하지는 않았지만, 데이터 제공부(230)는 키 분배 동작 이후에, 양자 통신 시스템(10) 내에서 암호화하여 교환하고자 하는 데이터를 발생할 수도 있다.
- [0064] 큐비트 발생부(240)는 제1 기저 그룹(BG1)에 기초하여 제1 큐비트 그룹(QG1)을 발생할 수 있다. 예를 들어, 큐비트 발생부(240)는 제1 기저 그룹(BG1)의 각 기저를 기초로 제1 데이터(DAT1)의 각 비트를 부호화하여 제1 큐비트 그룹(QG1)을 발생할 수 있으며, 상기 부호화 동작을 수행하기 위한 부호화부를 포함하여 구현될 수 있다. 예를 들어, 제1 데이터(DAT1)가 N비트의 이진 데이터이고 제1 기저 그룹(BG1)이 N개의 상기 제1 및 제2 기저들의 조합으로 이루어지는 경우에, 제1 큐비트 그룹(QG1)은 제1 내지 제N 큐비트들을 포함하는 데이터일 수 있다.
- [0065] 도 6에 도시된 것처럼, N이 10인 경우에 기초하여 제1 사용자 단말기(200)의 제1 큐비트 그룹(QG1)의 발생 동작을 설명할 수 있다. 예를 들어, 데이터 제공부(230)는 "0100101011"의 10비트의 제1 데이터(DAT1)를 발생할 수 있다. 큐비트 발생부(240)는 "+ + × + × × + × × +"의 제1 기저 그룹(BG1)을 기초로 "0100101011"의 제1 데이터(DAT1)를 부호화하여 제1 큐비트 그룹(QG1)을 발생할 수 있다. 제1 큐비트 그룹(QG1)은 제1 큐비트($|0\rangle$), 제2 큐비트($|1\rangle$), 제3 큐비트($|+\rangle$), 제4 큐비트($|0\rangle$), 제5 큐비트($|-\rangle$), 제6 큐비트($|+\rangle$), 제7 큐비트($|1\rangle$), 제8 큐비트($|+\rangle$), 제9 큐비트($|-\rangle$) 및 제10 큐비트($|1\rangle$)를 포함할 수 있다.
- [0066] 송수신부(250)는 제1 큐비트 그룹(QG1)을 서버(100)에 전송할 수 있고, 송수신부(110)는 제1 사용자 단말기(200)로부터 제1 큐비트 그룹(QG1)을 수신할 수 있다.
- [0067] 랜덤 넘버 발생부(120)는 랜덤 넘버(RN)를 발생할 수 있다. 예를 들어, 제1 랜덤 넘버(RN1)와 유사하게, 랜덤 넘버(RN)는 N비트의 임의의 이진 넘버일 수 있다. 랜덤 넘버 발생부(210)와 유사하게, 랜덤 넘버 발생부(120)는 임의의 랜덤 넘버 발생기를 포함하거나, 사용자 설정 신호에 기초하여 랜덤 넘버(RN)를 발생할 수도 있다. 예를 들어, 랜덤 넘버(RN)는 제1 사용자 단말기(200)에 의해 획득되는 복수의 키 비트들(KB1)과 실질적으로 동일할 수 있다.
- [0068] 리턴 큐비트 발생부(130)는 상기 제1 및 제2 게이트들을 기초로 제1 큐비트 그룹(QG1)에 포함되는 상기 제1 내지 제N 큐비트들 각각을 변경 또는 유지하여, 제1 리턴 큐비트 그룹(RQG1)을 발생할 수 있다. 예를 들어, 리턴 큐비트 발생부(130)는 랜덤 넘버(RN)를 기초로 상기 제1 내지 제N 큐비트들 각각에 상기 제1 및 제2 게이트들 중 하나를 적용하여, 제1 리턴 큐비트 그룹(RQG1)을 발생할 수 있다. 예를 들어, 제1 큐비트 그룹(QG1)과 유사하게, 제1 리턴 큐비트 그룹(RQG1)은 제1 내지 제N 리턴 큐비트들을 포함하는 데이터일 수 있고, 리턴 큐비트 발생부(130)는 랜덤 넘버(RN)의 제1 비트를 기초로 제1 큐비트 그룹(QG1)의 상기 제1 큐비트에 상기 제1 및 제2 게이트들 중 하나를 적용하여, 제1 리턴 큐비트 그룹(RQG1)의 상기 제1 리턴 큐비트를 발생할 수 있다. 리턴 큐비트 발생부(130)는 상기 제1 및 제2 게이트들을 포함하여 구현될 수 있다.
- [0069] 도 5a를 참조하면, 상기 제1 게이트는 파울리 X 게이트(Pauli X gate)를 나타낼 수 있다. 상기 파울리 X 게이트는, 상기 제1 큐비트가 상기 계산 기저에 기초하여 발생된 큐비트들(예를 들어, $|0\rangle$, $|1\rangle$) 중 하나인 경우에, 상기 제1 큐비트를 변경하기 위한 부정 게이트(NOT gate)로서 동작할 수 있다. 예를 들어, 큐비트($|0\rangle$)에 상기 파울리 X 게이트를 적용하면 큐비트($|1\rangle$)로 변경될 수 있고, 큐비트($|1\rangle$)에 상기 파울리 X 게이트를 적용하면 큐비트($|0\rangle$)로 변경될 수 있다. 상기 파울리 X 게이트는, 상기 제1 큐비트가 상기 하다마드 기저에 기초하여 발생된 큐비트들(예를 들어, $|+\rangle$, $|-\rangle$) 중 하나인 경우에, 상기 제1 큐비트를 변경하지 않고 유지시킬 수 있다. 예를 들어, 큐비트($|+\rangle$)에 상기 파울리 X 게이트를 적용하면 큐비트($|+\rangle$)가 유지될 수 있고, 큐비트($|-\rangle$)에 상기 파울리 X 게이트를 적용하면 큐비트($|-\rangle$)가 유지될 수 있다. 상기 파울리 X 게이트는 하기의 [수학식 1]과 같이 정의될 수 있다.

[0070] [수학식 1]

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

[0071]

[0072] 도 5b를 참조하면, 상기 제2 게이트는 파울리 Z 게이트(Pauli Z gate)를 나타낼 수 있다. 상기 파울리 Z 게이트는 상기 파울리 X 게이트와 반대로 동작할 수 있다. 상기 파울리 Z 게이트는, 상기 제1 큐비트가 상기 하다마드 기저에 기초하여 발생된 경우에, 상기 제1 큐비트를 변경하기 위한 상기 부정 게이트로서 동작할 수 있다. 예를 들어, 큐비트($|+\rangle$)에 상기 파울리 Z 게이트를 적용하면 큐비트($|-\rangle$)로 변경될 수 있고, 큐비트($|-\rangle$)에 상기 파울리 Z 게이트를 적용하면 큐비트($|+\rangle$)로 변경될 수 있다. 상기 파울리 Z 게이트는, 상기 제1 큐비트가 상기 계산 기저에 기초하여 발생된 경우에, 상기 제1 큐비트를 변경하지 않고 유지시킬 수 있다. 예를 들어, 큐비트($|0\rangle$)에 상기 파울리 Z 게이트를 적용하면 큐비트($|0\rangle$)가 유지될 수 있고, 큐비트($|1\rangle$)에 상기 파울리 Z 게이트를 적용하면 큐비트($|1\rangle$)가 유지될 수 있다. 상기 파울리 Z 게이트는 하기의 [수학식 2]와 같이 정의될 수 있다.

[0073] [수학식 2]

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

[0074]

[0075] 다시 도 3 및 6을 참조하면, 복수의 키 비트들(KB1)에 포함되는 제1 키 비트를 상기 제1 비트 값(예를 들어, "1")으로 설정하고자 하는 경우에, 리턴 큐비트 발생부(130)는 상기 제1 큐비트에 상기 제1 게이트를 적용하여 상기 제1 리턴 큐비트를 발생시킬 수 있다. 상기 제1 키 비트를 상기 제2 비트 값(예를 들어, "0")으로 설정하고자 하는 경우에, 리턴 큐비트 발생부(130)는 상기 제1 큐비트에 상기 제2 게이트를 적용하여 상기 제1 리턴 큐비트를 발생시킬 수 있다.

[0076] 일 실시예에서, 리턴 큐비트 발생부(130)는 랜덤 넘버(RN)에 기초하여 상기 제1 및 제2 게이트들의 적용 순서를 나타낼 수 있다. 예를 들어, 랜덤 넘버(RN)는 L(L은 0 이상 N 이하의 정수)개의 상기 제1 비트 값(예를 들어, "1")과 다른 (N-L)개의 상기 제2 비트 값(예를 들어, "0")의 조합으로 이루어지는 N비트의 이진 넘버일 수 있다. 리턴 큐비트 발생부(130)는 랜덤 넘버(RN)의 상기 제1 비트 값을 X(즉, 상기 제1 게이트를 적용하기 위한 값)로 변환하고 랜덤 넘버(RN)의 상기 제2 비트 값을 Z(즉, 상기 제2 게이트를 적용하기 위한 값)로 변환하여, N개의 상기 X 및 Z들의 조합으로 이루어지는 상기 제1 및 제2 게이트들의 적용 순서(SO)를 발생시킬 수 있다.

[0077] 도 6에 도시된 것처럼, N이 10인 경우에 기초하여 서버(100)의 제1 리턴 큐비트 그룹(RQG1)의 발생 동작을 설명할 수 있다. 예를 들어, 랜덤 넘버 발생부(120)는 "1011010100"의 10비트의 랜덤 넘버(RN)를 발생시킬 수 있다. 리턴 큐비트 발생부(130)는 "1011010100"의 랜덤 넘버(RN)에 기초하여 "XZXXZXZXZZ"의 상기 제1 및 제2 게이트들의 적용 순서(SO)를 발생시킬 수 있다. 리턴 큐비트 발생부(130)는 "XZXXZXZXZZ"의 상기 제1 및 제2 게이트들의 적용 순서(SO)를 기초로, 제1 큐비트 그룹(QG1)의 상기 제1, 제3, 제4, 제6 및 제8 큐비트들에 상기 제1 게이트를 적용하여 제1 리턴 큐비트 그룹(RQG1)의 상기 제1, 제3, 제4, 제6 및 제8 리턴 큐비트들을 발생시킬 수 있고, 제1 큐비트 그룹(QG1)의 상기 제2, 제5, 제7, 제9 및 제10 큐비트들에 상기 제2 게이트를 적용하여 제1 리턴 큐비트 그룹(RQG1)의 제2, 제5, 제7, 제9 및 제10 리턴 큐비트들을 발생시킬 수 있다.

[0078] 일 실시예에서, 상기 계산 기저에 기초하여 발생된 상기 제1 큐비트($|0\rangle$)와, 상기 제1 큐비트에 상기 파울리 X 게이트를 적용하여 발생된 상기 제1 리턴 큐비트($|1\rangle$)는, 서로 다른 값을 가질 수 있다. 상기 하다마드 기저에 기초하여 발생된 상기 제3 큐비트($|+\rangle$)와, 상기 제3 큐비트에 상기 파울리 X 게이트를 적용하여 발생된 상기 제3 리턴 큐비트($|+\rangle$)는, 동일한 값을 가질 수 있다. 상기 계산 기저에 기초하여 발생된 상기 제2 큐비트($|1\rangle$)와, 상기 제2 큐비트에 상기 파울리 Z 게이트를 적용하여 발생된 상기 제2 리턴 큐비트($|1\rangle$)는, 동일한 값을 가질 수 있다. 상기 하다마드 기저에 기초하여 발생된 상기 제5 큐비트($|-\rangle$)와, 상기 제5 큐비트에 상기 파울리 Z 게이트를 적용하여 발생된 상기 제5 리턴 큐비트($|+\rangle$)는, 서로 다른 값을 가질 수 있다.

[0079] 송수신부(110)는 제1 리턴 큐비트 그룹(RQG1)을 제1 사용자 단말기(200)에 전송할 수 있고, 송수신부(250)는 서버(100)로부터 제1 리턴 큐비트 그룹(RQG1)을 수신할 수 있다.

[0080] 키 발생부(260)는 제1 큐비트 그룹(QG1)과 제1 리턴 큐비트 그룹(RQG1)을 비교하여 복수의 키 비트들(KB1)을 획득할 수 있다. 예를 들어, 키 발생부(260)는 제1 큐비트 그룹(QG1)의 상기 제1 큐비트와 제1 리턴 큐비트 그룹

(RQG1)의 상기 제1 리턴 큐비트가 동일한지 여부, 및 상기 제1 큐비트의 발생 시에 사용된 기저의 종류에 기초하여, 복수의 키 비트들(KB1)의 상기 제1 키 비트를 획득할 수 있다. 예를 들어, 랜덤 넘버(RN)와 동일하게, 복수의 키 비트들(KB1)은 N비트의 이진 넘버일 수 있다.

[0081] 도 6에 도시된 것처럼, N이 10인 경우에 기초하여 제1 사용자 단말기(200)의 복수의 키 비트들(KB1)의 발생 동작을 설명할 수 있다. 예를 들어, 키 발생부(260)는 상기 제1 내지 제10 큐비트들과 상기 제1 내지 제10 리턴 큐비트들을 비교하고 제1 기저 그룹(BG1)에 기초하여 복수의 키 비트들(KB1)을 획득할 수 있다. 예를 들어, 상기 계산 기저에 기초하여 발생된 상기 제1 큐비트($|0\rangle$)와 상기 제1 리턴 큐비트($|1\rangle$)가 서로 다른 값을 가지므로, 상기 제1 키 비트는 상기 제1 게이트에 상응하는 상기 제1 비트 값(예를 들어, "1")으로 판단될 수 있다. 상기 계산 기저에 기초하여 발생된 상기 제2 큐비트($|1\rangle$)와 상기 제2 리턴 큐비트($|1\rangle$)가 동일한 값을 가지므로, 제2 키 비트는 상기 제2 게이트에 상응하는 상기 제2 비트 값(예를 들어, "0")으로 판단될 수 있다. 상기 하다마드 기저에 기초하여 발생된 상기 제3 큐비트($|+\rangle$)와 상기 제3 리턴 큐비트($|+\rangle$)가 동일한 값을 가지므로, 제3 키 비트는 상기 제1 게이트에 상응하는 상기 제1 비트 값(예를 들어, "1")으로 판단될 수 있다. 상기 하다마드 기저에 기초하여 발생된 상기 제5 큐비트($|-\rangle$)와 상기 제5 리턴 큐비트($|+\rangle$)가 서로 다른 값을 가지므로, 제5 키 비트는 상기 제2 게이트에 상응하는 상기 제2 비트 값(예를 들어, "0")으로 판단될 수 있다.

[0082] 채널(202)은 상기 양자 채널 또는 상기 보안 채널일 수 있고, 채널(204)은 상기 고전 채널 또는 상기 공개 채널일 수 있다. 채널(202)을 통해 제1 큐비트 그룹(QG1) 및 제1 리턴 큐비트 그룹(RQG1)이 전송될 수 있다. 예를 들어, 채널(204)은 TCP/IP 프로토콜에 기초하여 동작할 수 있다.

[0083] 일 실시예에서, 서버(100) 및 제1 사용자 단말기(200)의 구성요소들의 일부 또는 전부는 프로그램(즉, 소프트웨어) 또는 하드웨어의 형태로 구현될 수 있다.

[0084] 도시하지는 않았지만, 서버(100) 및 제1 사용자 단말기(200)는, 특정 계산들 또는 태스크들과 같은 다양한 컴퓨팅 기능들을 실행하는 프로세서, 상기 프로세서에 의해 처리되는 데이터, 명령어 등을 저장하는 메모리 또는 저장부, 도 8을 참조하여 후술하는 정보 조정(information reconciliation) 및 비밀성 증폭(privacy amplification)을 수행하기 위한 후처리부, 도 8을 참조하여 후술하는 보안 통신을 수행하기 위한 부호화부 및 복호화부 등을 더 포함하여 구현될 수 있다.

[0085] 도 7을 참조하면, 서버(100)와 제2 사용자 단말기(300)의 키 분배 동작은 도 3 내지 6을 참조하여 상술한 서버(100)와 제1 사용자 단말기(200)의 키 분배 동작과 실질적으로 동일할 수 있다. 제1 사용자 단말기(200)와 유사하게, 제2 사용자 단말기(300)는 랜덤 넘버 발생부, 기저 결정부, 데이터 제공부, 큐비트 발생부, 송수신부 및 키 발생부를 포함할 수 있다.

[0086] 제2 사용자 단말기(300)는 상기 제1 및 제2 기저들의 조합으로 이루어지는 제2 기저 그룹(BG2)을 발생할 수 있고, 제2 기저 그룹(BG2)에 기초하여 제2 큐비트 그룹(QG2)을 발생할 수 있다. 예를 들어, 도 7에 도시된 것처럼, "0101010010"의 제1 랜덤 넘버(RN1)에 기초하여 " $\times + \times + \times + \times + \times + \times$ "의 제2 기저 그룹(BG2)이 발생될 수 있고, " $\times + \times + \times + \times + \times + \times$ "의 제2 기저 그룹(BG2)을 기초로 "1010001001"의 제2 데이터를 부호화하여 제2 큐비트 그룹(QG2)을 발생할 수 있다.

[0087] 서버(100)는 제2 큐비트 그룹(QG2)에 포함되는 각 큐비트에 상기 제1 및 제2 게이트들 중 하나를 적용하여, 제2 리턴 큐비트 그룹(RQG2)을 발생할 수 있다. 예를 들어, 도 7에 도시된 것처럼, "XZXXZXZXZZ"의 상기 제1 및 제2 게이트들의 적용 순서(S0)를 기초로, 제2 큐비트 그룹(QG2)의 제1, 제3, 제4, 제6 및 제8 큐비트들에 상기 제1 게이트를 적용하고 제2 큐비트 그룹(QG2)의 제2, 제5, 제7, 제9 및 제10 큐비트들에 상기 제2 게이트를 적용하여, 제2 리턴 큐비트 그룹(RQG2)을 발생할 수 있다.

[0088] 제2 사용자 단말기(300)는 제2 큐비트 그룹(QG2)과 제2 리턴 큐비트 그룹(RQG2)을 비교하여 복수의 키 비트들(KB2)을 획득할 수 있다.

[0089] 상술한 것처럼, 제1 사용자 단말기(200)에 의해 생성된 제1 큐비트 그룹(QG1)과 제2 사용자 단말기(300)에 의해 생성된 제2 큐비트 그룹(QG2)은 서로 상이할 수 있으나, 서버(100)가 큐비트 그룹들(QG1, QG2)에 동일한 순서(S0)로 상기 제1 및 제2 게이트들을 적용하기 때문에, 사용자 단말기들(200, 300)에 전송되는 리턴 큐비트 그룹들(RQG1, RQG2)은 상기 키 비트들과 관련된 동일한 정보를 포함할 수 있다. 따라서, 제1 사용자 단말기(200)에 의해 획득되는 복수의 키 비트들(KB1)과 제2 사용자 단말기(300)에 의해 획득되는 복수의 키 비트들(KB2)은 실질적으로 동일할 수 있다.

- [0090] 도시하지는 않았으나, 서버(100)와 나머지 사용자 단말기들(400, 500)의 키 분배 동작 역시 도 3 내지 6을 참조하여 상술한 서버(100)와 제1 사용자 단말기(200)의 키 분배 동작과 실질적으로 동일할 수 있다.
- [0091] 일 실시예에서, 사용자 단말기들(200, 300, 400, 500) 각각에 대해 키 분배 동작이 순차적으로 수행될 수 있다. 예를 들어, 제1 사용자 단말기(200)에 대해 도 3의 단계 S100~S400이 수행될 수 있고, 이후에 제2 사용자 단말기(300)에 대해 도 3의 단계 S100~S400이 수행될 수 있으며, 이후에 제3 사용자 단말기(400)에 대해 도 3의 단계 S100~S400이 수행될 수 있으며, 이후에 제4 사용자 단말기(500)에 대해 도 3의 단계 S100~S400이 수행될 수 있다.
- [0092] 다른 실시예에서, 사용자 단말기들(200, 300, 400, 500) 모두에 대해 키 분배 동작이 실질적으로 동시에 수행될 수 있다. 예를 들어, 사용자 단말기들(200, 300, 400, 500)에 대해 도 3의 단계 S100이 수행될 수 있고, 이후에 사용자 단말기들(200, 300, 400, 500)에 대해 도 3의 단계 S200이 수행될 수 있고, 이후에 사용자 단말기들(200, 300, 400, 500)에 대해 도 3의 단계 S300이 수행될 수 있으며, 이후에 사용자 단말기들(200, 300, 400, 500)에 대해 도 3의 단계 S400이 수행될 수 있다.
- [0093] 도 8은 본 발명의 실시예들에 따른 양자 통신 방법을 나타내는 순서도이다.
- [0094] 도 1 및 8을 참조하면, 본 발명의 실시예들에 따른 양자 통신 방법에서, 복수의 사용자 단말기들(200, 300, 400, 500)은 복수의 기저 그룹들을 발생하고(단계 S1100), 사용자 단말기들(200, 300, 400, 500)은 상기 복수의 기저 그룹들을 기초로 복수의 큐비트 그룹들을 발생하여 서버(100)에 전송하고(단계 S1200), 서버(100)는 제 1 및 제2 게이트들을 기초로, 상기 복수의 큐비트 그룹들에 포함되는 복수의 큐비트들 각각을 변경 또는 유지하여 복수의 리턴 큐비트 그룹들을 발생하고, 상기 복수의 리턴 큐비트 그룹들을 사용자 단말기들(200, 300, 400, 500)에 전송하며(단계 S1300), 사용자 단말기들(200, 300, 400, 500)은 상기 복수의 큐비트 그룹들과 상기 복수의 리턴 큐비트 그룹들을 비교하여, 복수의 키 비트들을 획득한다(단계 S1400). 도 8의 단계 S1100 내지 S1400은 도 3의 단계 S100 내지 S400과 각각 실질적으로 동일할 수 있다.
- [0095] 서버(100) 및 사용자 단말기들(200, 300, 400, 500)은 상기 복수의 키 비트들에 대한 정보 조정 및 비밀성 증폭을 수행하여, 보안 키를 공유한다(단계 S1500). 서버(100) 및 사용자 단말기들(200, 300, 400, 500)은 상기 보안 키를 기초로 데이터를 암호화하여 교환한다(단계 S1600).
- [0096] 상기 정보 조정은 상기 보안 키의 동일성을 확보하기 위한 동작일 수 있다. 구체적으로, 노이즈 및/또는 간섭 등에 의해 서버(100)에서 전송된 상기 복수의 키 비트들과, 사용자 단말기들(200, 300, 400, 500)에서 수신된 상기 복수의 키 비트들 사이에 발생하는 불일치(예를 들어, 채널 오류 또는 제3자의 도청에 의한 오류)가, 상기 정보 조정에 의해 해소될 수 있다. 예를 들어, 상기 불일치를 조정하기 위해 오류 정정 코드가 사용될 수 있으며, 따라서 상기 정보 조정을 오류 정정(error correction)이라 부를 수도 있다.
- [0097] 상기 비밀성 증폭은 상기 복수의 키 비트들에서 제3자(third party)에게 누설된 정보를 제거하기 위한 동작일 수 있다. 구체적으로, 상기 비밀성 증폭은 서버(100)와 사용자 단말기들(200, 300, 400, 500)이 공통된 상기 보안 키를 획득하는 과정에서 제3자에게 누설된 정보를 제거하는 동작을 나타낼 수 있다. 상기 비밀성 증폭에 의해 상기 보안 키의 길이가 상기 복수의 키 비트들의 길이보다 감소될 수 있지만, 상기 보안 키의 랜덤성, 보안성, 안전성 및/또는 기밀성이 확보될 수 있다.
- [0098] 상기와 같은 정보 조정 및 비밀성 증폭은 양자 후처리(post-process) 기술일 수 있으며, 서버(100) 및 사용자 단말기들(200, 300, 400, 500) 내부의 별도의 후처리부(미도시)에 의해 수행될 수 있다. 상기 정보 조정 및 상기 비밀성 증폭에 의해, 서버(100)와 사용자 단말기들(200, 300, 400, 500)이 실질적으로 동일한 상기 보안 키를 안전하게 공유할 수 있다.
- [0099] 일 실시예에서, 상기 복수의 큐비트 그룹들 및 상기 복수의 리턴 큐비트 그룹들은, 서버(100)와 사용자 단말기들(200, 300, 400, 500) 사이의 양자 채널(예를 들어, 도 1의 실선 화살표)을 통해 전송될 수 있다. 상기 정보 조정 및 상기 비밀성 증폭은, 서버(100)와 사용자 단말기들(200, 300, 400, 500) 사이의 공개 채널(예를 들어, 도 1의 점선 화살표)을 통해 수행될 수 있다.
- [0100] 상기 복수의 키 비트들은 로우 키(raw key) 또는 선별 키(sifted key)라고 불릴 수 있고, 상기 보안 키는 최종 키(final key)로 불릴 수 있다. 키 분배 동작 이후에 실제 데이터 교환 동작은 최종 키인 상기 보안 키에 기초하여 수행될 수 있다.
- [0101] 일 실시예에서, 상기 보안 키의 비트 수는 상기 복수의 키 비트들의 수보다 적을 수 있다. 예를 들어, 상기 비

밀성 증폭에 의해 상기 보안 키가 상대적으로 적은 비트 수를 가질 수 있다. 다만, 상기 보안 키의 비트 수가 증가할수록 유리하며, 예를 들어 상기 보안 키의 비트 수가 증가할수록 보안 통신의 성능 및 정확도가 향상될 수 있다.

[0102] 일 실시예에서, 단계 S1600에서 교환되는 상기 데이터는 상기 보안 키를 이용하는 원타임 패드(one-time pad) 방식에 의해 암호화될 수 있다. 다만, 상기 데이터의 암호화 방식은 실시예에 따라서 다양하게 변경될 수 있다.

[0103] 본 발명의 실시예들에 따른 양자 통신 방법에서는, 서버(100)가 큐비트들을 직접 발생하지 않고, 사용자 단말기들(200, 300, 400, 500)에서 발생된 큐비트들에 상기 제1 및 제2 게이트들을 선택적으로 적용한 후에 상기 큐비트들을 사용자 단말기들(200, 300, 400, 500)에 되돌려줌으로써, 상기 키 비트들과 관련된 정보를 사용자 단말기들(200, 300, 400, 500)에 전송할 수 있다. 따라서, 서버(100)의 부하(load)가 감소될 수 있으며, 사용자 단말기들(200, 300, 400, 500)이 동일한 키 비트들을 효율적으로 공유할 수 있다. 또한, 상기 정보 조정 및 상기 비밀성 증폭이 수행되는 경우에만 공개 채널이 사용되므로, 상기 보안 키 생성을 위한 공개 채널의 사용이 감소될 수 있으며, 얽힘(entanglement) 및 양자 메모리(quantum memory)의 사용이 불필요할 수 있다.

[0104] 본 발명의 실시예들에 따른 양자 통신에서의 다자간 키 교환 방법 및/또는 양자 통신 방법은 임의의 모바일 기기 또는 임의의 컴퓨팅 시스템에 적용될 수 있으며, 본 발명의 실시예들에 따른 양자 통신 시스템에 포함되는 서버 및 사용자 단말기들은 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.

[0105] 본 발명의 실시예들에 따른 양자 통신에서의 다자간 키 교환 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.

[0106] 이상, 전자의 회전 상태를 이용하여 신호를 전송하는 양자 통신 방식에 기초하여 본 발명의 실시예들을 상세하게 설명하였으나, 본 발명의 실시예들은 광자(photon)의 편광 상태(polarization)를 이용하거나 위상차를 이용하여 신호를 전송하는 양자 통신 방식에 대해서도 적용될 수 있다.

산업상 이용가능성

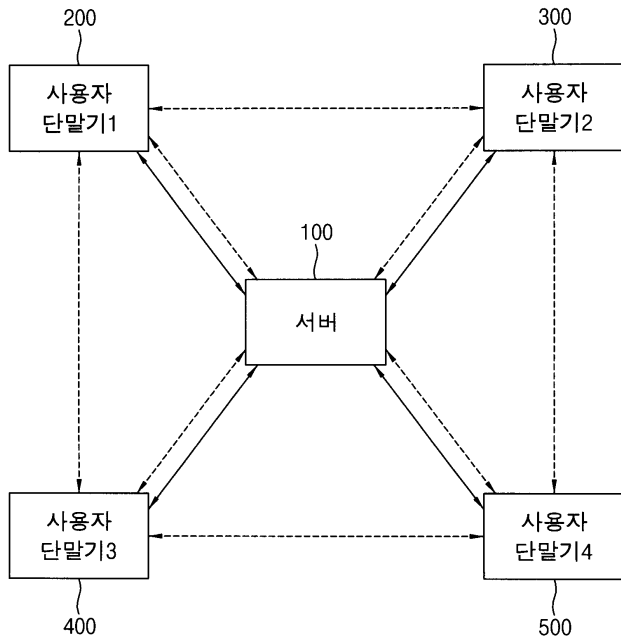
[0107] 본 발명은 다양한 통신 장치 및 통신 시스템에 적용될 수 있다. 따라서 본 발명은 휴대폰, 스마트 폰, PDA, PMP, 디지털 카메라, 캠코더, PC, 서버 컴퓨터, 워크스테이션, 노트북, 디지털 TV, 셋-탑 박스, 음악 재생기, 휴대용 게임 콘솔, 네비게이션 시스템, 스마트 카드, 프린터 등과 같은 다양한 전자 기기에 유용하게 이용될 수 있다.

[0108] 상기에서는 본 발명의 바람직한 실시예를 참조하여 설명하였지만, 해당 기술분야의 숙련된 당업자는 하기의 특허청구범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 것이다.

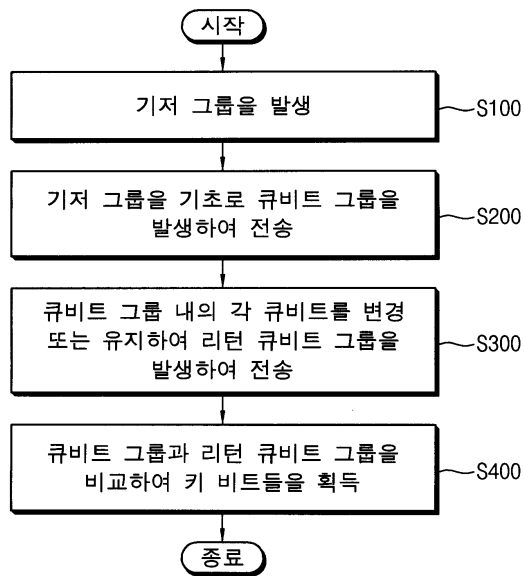
도면

도면1

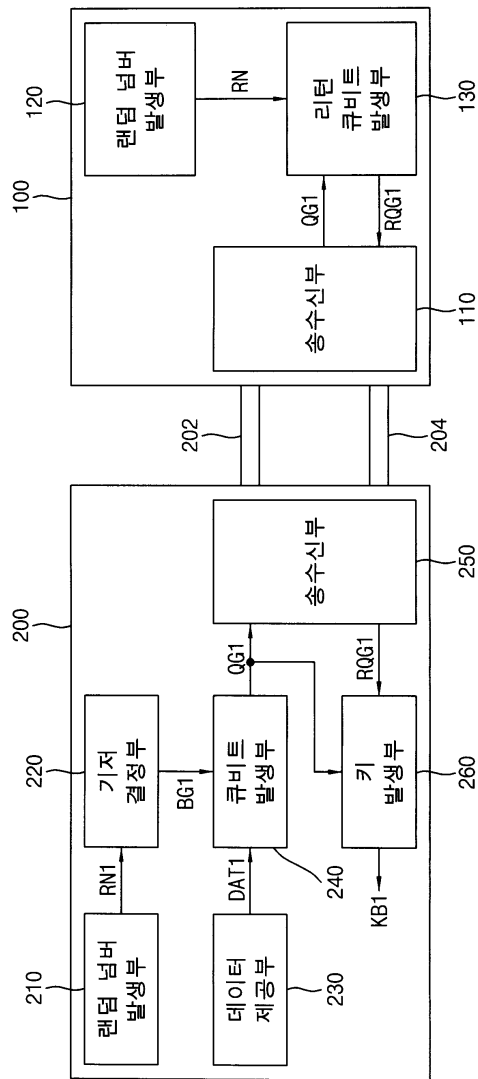
10



도면2



도면3



도면4

	스핀 다운	스핀 업
+	$ 0\rangle$	$ 1\rangle$
x	$ +\rangle$	$ -\rangle$

도면5a

	파울리 X 게이트 적용 후
$ 0\rangle$	$ 1\rangle$
$ 1\rangle$	$ 0\rangle$
$ +\rangle$	$ +\rangle$
$ -\rangle$	$ -\rangle$

도면5b

	파울리 Z 게이트 적용 후
$ 0\rangle$	$ 0\rangle$
$ 1\rangle$	$ 1\rangle$
$ +\rangle$	$ -\rangle$
$ -\rangle$	$ +\rangle$

도면6

큐비트#	1	2	3	4	5	6	7	8	9	10
BG1	+	+	x	+	x	x	+	x	x	+
QG1	$ 0\rangle$	$ 1\rangle$	$ +\rangle$	$ 0\rangle$	$ -\rangle$	$ +\rangle$	$ 1\rangle$	$ +\rangle$	$ -\rangle$	$ 1\rangle$
S0	x	Z	x	x	Z	x	Z	x	Z	Z
RQG1	$ 1\rangle$	$ 1\rangle$	$ +\rangle$	$ 1\rangle$	$ +\rangle$	$ +\rangle$	$ 1\rangle$	$ +\rangle$	$ +\rangle$	$ 1\rangle$
KB1	1	0	1	1	0	1	0	1	0	0

도면7

큐비트#	1	2	3	4	5	6	7	8	9	10
BG2	x	+	x	+	x	+	x	x	+	x
QG2	$\downarrow$ $\rangle$	$0\rangle$	$1\rangle$	$0\rangle$	$1\rangle$	$0\rangle$	$\downarrow$ $\rangle$	$1\rangle$	$0\rangle$	$\downarrow$ $\rangle$
S0	x	Z	x	x	Z	x	Z	x	Z	Z
RQG2	$\downarrow$ $\rangle$	$0\rangle$	$0\rangle$	$1\rangle$	$\downarrow$ $\rangle$	$1\rangle$	$1\rangle$	$1\rangle$	$0\rangle$	$1\rangle$
KB2	1	0	1	1	0	1	0	1	0	0

도면8

