(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2017-0126156
(43) 공개일자 2017년11월17일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *H04L 1/00* (2006.01)
H04L 1/24 (2006.01)
(52) CPC특허분류
H04L 9/0852 (2013.01)
H04L 1/0042 (2013.01)
(21) 출원번호 10-2016-0056189
(22) 출원일자 2016년05월09일
심사청구일자 2016년05월09일

(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

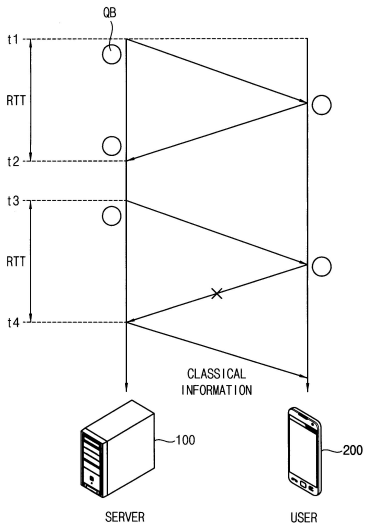
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 **저 전력 양자 키 분배 방법, 이를 이용한 양자 통신 방법 및 이를 수행하는 양자 통신 시스템**

(57) 요 약

양자 키 분배 방법은 서버가 큐빗을 생성하여 상기 큐빗을 유저 단말로 전송하는 단계, 시큐리티 체크 모드가 아닐 때, 상기 유저 단말이 상기 큐빗 상에 시크릿 키를 인코딩하여 상기 시크릿 키가 인코딩된 상기 큐빗을 상기 서버로 루프백하는 단계, 상기 시큐리티 체크 모드일 때, 상기 유저 단말이 상기 큐빗을 측정하는 단계 및 상기 서버가 상기 큐빗을 루프백 받지 못한 경우, 상기 서버가 상기 큐빗이 정확한 기저에 의해 측정될 때의 측정 결과를 상기 유저 단말에 전송하는 단계를 포함한다.

대 표 도 - 도1



(52) CPC특허분류
H04L 1/243 (2013.01)
H04L 9/0819 (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

명 세 서

청구범위

청구항 1

서버가 큐빗을 생성하여 상기 큐빗을 유저 단말로 전송하는 단계;

시큐리티 체크 모드가 아닐 때, 상기 유저 단말이 상기 큐빗 상에 시크릿 키를 인코딩하여 상기 시크릿 키가 인코딩된 상기 큐빗을 상기 서버로 루프백하는 단계;

상기 시큐리티 체크 모드일 때, 상기 유저 단말이 상기 큐빗을 측정하는 단계; 및

상기 서버가 상기 큐빗을 루프백 받지 못한 경우, 상기 서버가 상기 큐빗이 정확한 기저에 의해 측정될 때의 측정 결과를 상기 유저 단말에 전송하는 단계를 포함하는 양자 키 분배 방법.

청구항 2

제1항에 있어서, 상기 유저 단말은 상기 큐빗 상에 상기 시크릿 키를 인코딩할 때, I-gate 및 Pauli Y-gate를 이용하고,

상기 I-gate는 $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ 이고,

상기 Pauli Y-gate는 $Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$ 인 것을 특징으로 하는 양자 키 분배 방법.

청구항 3

제2항에 있어서, 0을 인코딩하기 위해서 상기 유저 단말은 상기 I-gate를 이용하고,

1을 인코딩하기 위해서 상기 유저 단말은 상기 Pauli Y-gate를 이용하는 것을 특징으로 하는 양자 키 분배 방법.

청구항 4

제1항에 있어서, 상기 큐빗은 광자(Photon)에 의해 전송되고,

상기 광자는 제1 및 제2 상태를 포함하고, 상기 광자는 제1 및 제2 기저(Basis)를 포함하는 것을 특징으로 하는 양자 키 분배 방법.

청구항 5

제4항에 있어서, 상기 제1 상태는 0이고,

상기 제2 상태는 1이며,

상기 제1 기저는 수평 방향의 제1 축 및 수직 방향의 제2 축을 갖는 X 기저이고,

상기 제2 기저는 제1 대각 방향의 제3 축 및 상기 제1 대각 방향과 수직한 제2 대각 방향의 제4 축을 갖는 Z 기저인 것을 특징으로 하는 양자 키 분배 방법.

청구항 6

제1항에 있어서, 상기 큐빗은 전자(Electron)에 의해 전송되고,

상기 전자는 제1 및 제2 상태를 포함하고, 상기 전자는 제1 및 제2 기저를 포함하는 것을 특징으로 하는 양자 키 분배 방법.

청구항 7

제1항에 있어서, 상기 유저 단말이 측정한 상기 큐빗의 제1 측정 결과 및 상기 서버가 전송한 상기 큐빗이 정확한 기저에 의해 측정될 때의 제2 측정 결과를 기초로 상기 유저 단말이 큐빗 측정의 에러율을 계산하는 단계를 더 포함하는 것을 특징으로 하는 양자 키 분배 방법.

청구항 8

제7항에 있어서, 상기 큐빗 측정의 상기 에러율이 기준 값보다 작으면 양자 키 분배가 계속 수행되고,

상기 큐빗 측정의 상기 에러율이 기준 값보다 크거가 같은 경우, 상기 양자 키 분배가 중단되는 것을 특징으로 하는 양자 키 분배 방법.

청구항 9

제1항에 있어서, 상기 시크릿 키의 비트 수가 증가하더라도 상기 유저 단말이 상기 서버로 발송하는 데이터의 비트 수는 일정한 것을 특징으로 하는 양자 키 분배 방법.

청구항 10

서버가 큐빗을 생성하여 상기 큐빗을 유저 단말로 전송하는 단계;

시큐리티 체크 모드가 아닐 때, 상기 유저 단말이 상기 큐빗 상에 시크릿 키를 인코딩하여 상기 시크릿 키가 인코딩된 상기 큐빗을 상기 서버로 루프백하는 단계;

상기 시큐리티 체크 모드일 때, 상기 유저 단말이 상기 큐빗을 측정하는 단계;

상기 서버가 상기 큐빗을 루프백 받지 못한 경우, 상기 서버가 상기 큐빗이 정확한 기저에 의해 측정될 때의 측정 결과를 상기 유저 단말에 전송하는 단계;

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

상기 서버와 상기 유저 단말이 상기 보안 키를 기초로 데이터를 암호화하여 교환하는 단계를 포함하는 양자 통신 방법.

청구항 11

큐빗을 생성하여 상기 큐빗을 유저 단말로 전송하고, 상기 큐빗을 상기 유저 단말로부터 루프백 받지 못한 경우 상기 큐빗이 정확한 기저에 의해 측정될 때의 측정 결과를 상기 유저 단말에 전송하는 서버; 및

시큐리티 체크 모드가 아닐 때, 상기 큐빗 상에 시크릿 키를 인코딩하여 상기 시크릿 키가 인코딩된 상기 큐빗을 상기 서버로 루프백하고, 상기 시큐리티 체크 모드일 때, 상기 큐빗을 측정하는 유저 단말을 포함하는 양자 통신 시스템.

청구항 12

제11항에 있어서, 상기 유저 단말이 저 전력 모드일 때 상기 서버가 상기 큐빗을 생성하고,

상기 유저 단말이 저 전력 모드가 아닐 때 상기 유저 단말이 상기 큐빗을 생성하는 것을 특징으로 하는 양자 통신 시스템.

청구항 13

제11항에 있어서, 상기 유저 단말은 상기 큐빗 상에 상기 시크릿 키를 인코딩할 때, I-gate 및 Pauli Y-gate를 이용하고,

상기 I-gate는 $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$이고,

상기 Pauli Y-gate는 $Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$ 인 것을 특징으로 하는 양자 통신 시스템.

청구항 14

제13항에 있어서, 0을 인코딩하기 위해서 상기 유저 단말은 상기 I-gate를 이용하고,

1을 인코딩하기 위해서 상기 유저 단말은 상기 Pauli Y-gate를 이용하는 것을 특징으로 하는 양자 통신 시스템.

청구항 15

제11항에 있어서, 상기 큐빗은 광자(Photon)에 의해 전송되고,

상기 광자는 제1 및 제2 상태를 포함하고, 상기 광자는 제1 및 제2 기저(Basis)를 포함하는 것을 특징으로 하는 양자 통신 시스템.

청구항 16

제15항에 있어서, 상기 제1 상태는 0이고,

상기 제2 상태는 1이며,

상기 제1 기저는 수평 방향의 제1 축 및 수직 방향의 제2 축을 갖는 X 기저이고,

상기 제2 기저는 제1 대각 방향의 제3 축 및 상기 제1 대각 방향과 수직한 제2 대각 방향의 제4 축을 갖는 Z 기저인 것을 특징으로 하는 양자 통신 시스템.

청구항 17

제11항에 있어서, 상기 큐빗은 전자(Electron)에 의해 전송되고,

상기 전자는 제1 및 제2 상태를 포함하고, 상기 전자는 제1 및 제2 기저를 포함하는 것을 특징으로 하는 양자 통신 시스템.

청구항 18

제11항에 있어서, 상기 유저 단말이 측정한 상기 큐빗의 제1 측정 결과 및 상기 서버가 전송한 상기 큐빗이 정확한 기저에 의해 측정될 때의 제2 측정 결과를 기초로 상기 유저 단말이 큐빗 측정의 에러율을 계산하는 단계를 더 포함하는 것을 특징으로 하는 양자 통신 시스템.

청구항 19

제18항에 있어서, 상기 큐빗 측정의 상기 에러율이 기준 값보다 작으면 양자 키 분배가 계속 수행되고,

상기 큐빗 측정의 상기 에러율이 기준 값보다 크거나 같은 경우, 상기 양자 키 분배가 중단되는 것을 특징으로 하는 양자 통신 시스템.

청구항 20

제11항에 있어서, 상기 유저 단말은 상기 큐빗을 상기 서버로 루프백하는 복수의 미러를 포함하는 것을 특징으로 하는 양자 통신 시스템.

발명의 설명

기 술 분 야

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

배 경 기 술

[0002] 1984년 C. H. Bennett과 G. Brassard에 의해 고안된 양자 키 분배(quantum key distribution: QKD) 프로토콜은 BB84 프로토콜로 불릴 수 있다. 상기와 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] 서버 및 유저 단말의 양자 키 분배를 위해서는 서버 및 유저 단말 중 어느 하나가 큐빗을 생성하여야 한다. 상기 큐빗을 생성하는 데에는 상대적으로 큰 전력이 필요하다.

[0004] 종래의 양자 키 분배 방식에서는 상기 유저 단말의 배터리가 매우 적을 때 상기 양자 키 분배가 이루어지지 못하는 문제가 있다.

발명의 내용

해결하려는 과제

[0005] 본 발명이 이루고자 하는 목적은 유저 단말의 전력 소비를 감소시켜 유저 단말의 배터리가 매우 적을 때에도 동작 가능한 양자 키 분배 방법을 제공하는 것이다.

[0006] 본 발명이 이루고자 하는 다른 목적은 상기 양자 키 분배 방법을 이용하는 양자 통신 방법을 제공하는 것이다.

[0007] 본 발명이 이루고자 하는 또 다른 목적은 상기 양자 키 분배 방법 및 상기 양자 통신 방법을 수행하는 양자 통신 시스템을 제공하는 것이다.

과제의 해결 수단

[0008] 상기한 본 발명의 목적을 실현하기 위한 일 실시예에 따른 양자 키 분배 방법은 서버가 큐빗을 생성하여 상기 큐빗을 유저 단말로 전송하는 단계, 시큐리티 체크 모드가 아닐 때, 상기 유저 단말이 상기 큐빗 상에 시크릿 키를 인코딩하여 상기 시크릿 키가 인코딩된 상기 큐빗을 상기 서버로 루프백하는 단계, 상기 시큐리티 체크 모드일 때, 상기 유저 단말이 상기 큐빗을 측정하는 단계 및 상기 서버가 상기 큐빗을 루프백 받지 못한 경우, 상기 서버가 상기 큐빗이 정확한 기저에 의해 측정될 때의 측정 결과를 상기 유저 단말에 전송하는 단계를 포함한다.

[0009] 본 발명의 일 실시예에 있어서, 상기 유저 단말은 상기 큐빗 상에 상기 시크릿 키를 인코딩할 때, I-gate 및 Pauli Y-gate를 이용할 수 있다. 상기 I-gate는 $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$일 수 있다. 상기 Pauli Y-gate는 $Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$일 수 있다.

[0010] 본 발명의 일 실시예에 있어서, 0을 인코딩하기 위해서 상기 유저 단말은 상기 I-gate를 이용할 수 있다. 1을 인코딩하기 위해서 상기 유저 단말은 상기 Pauli Y-gate를 이용할 수 있다.

[0011] 본 발명의 일 실시예에 있어서, 상기 큐빗은 광자(Photon)에 의해 전송될 수 있다. 상기 광자는 제1 및 제2 상태를 포함하고, 상기 광자는 제1 및 제2 기저(Basis)를 포함할 수 있다.

[0012] 본 발명의 일 실시예에 있어서, 상기 제1 상태는 0일 수 있다. 상기 제2 상태는 1일 수 있다. 상기 제1 기저는 수평 방향의 제1 축 및 수직 방향의 제2 축을 갖는 X 기저일 수 있다. 상기 제2 기저는 제1 대각 방향의 제3 축 및 상기 제1 대각 방향과 수직한 제2 대각 방향의 제4 축을 갖는 Z 기저일 수 있다.

[0013] 본 발명의 일 실시예에 있어서, 상기 큐빗은 전자(Electron)에 의해 전송될 수 있다. 상기 전자는 제1 및 제2 상태를 포함하고, 상기 전자는 제1 및 제2 기저를 포함할 수 있다.

[0014] 본 발명의 일 실시예에 있어서, 상기 양자 키 분배 방법은 상기 유저 단말이 측정한 상기 큐빗의 제1 측정 결과 및 상기 서버가 전송한 상기 큐빗이 정확한 기저에 의해 측정될 때의 제2 측정 결과를 기초로 상기 유저 단말이 큐빗 측정의 에러율을 계산하는 단계를 더 포함할 수 있다.

[0015] 본 발명의 일 실시예에 있어서, 상기 큐빗 측정의 상기 에러율이 기준 값보다 작으면 양자 키 분배가 계속 수행

될 수 있다. 상기 큐빗 측정의 상기 에러율이 기준 값보다 크거가 같은 경우, 상기 양자 키 분배가 중단될 수 있다.

[0016] 본 발명의 일 실시예에 있어서, 상기 시크릿 키의 비트 수가 증가하더라도 상기 유저 단말이 상기 서버로 발송하는 데이터의 비트 수는 일정할 수 있다.

[0017] 상기한 본 발명의 목적을 실현하기 위한 일 실시예에 따른 양자 통신 방법은 서버가 큐빗을 생성하여 상기 큐빗을 유저 단말로 전송하는 단계, 시큐리티 체크 모드가 아닐 때, 상기 유저 단말이 상기 큐빗 상에 시크릿 키를 인코딩하여 상기 시크릿 키가 인코딩된 상기 큐빗을 상기 서버로 루프백하는 단계, 상기 시큐리티 체크 모드일 때, 상기 유저 단말이 상기 큐빗을 측정하는 단계, 상기 서버가 상기 큐빗을 루프백 받지 못한 경우, 상기 서버가 상기 큐빗이 정확한 기저에 의해 측정될 때의 측정 결과를 상기 유저 단말에 전송하는 단계, 상기 서버 및 상기 유저 단말이, 복수의 상기 시크릿 키 비트들에 대한 정보 조정(information reconciliation) 및 비밀성 증폭(privacy amplification)을 수행하여, 보안 키를 공유하는 단계 및 상기 서버와 상기 유저 단말이 상기 보안 키를 기초로 데이터를 암호화하여 교환하는 단계를 포함한다.

[0018] 상기한 본 발명의 목적을 실현하기 위한 일 실시예에 따른 양자 통신 시스템은 서버 및 유저 단말을 포함한다. 상기 서버는 큐빗을 생성하여 상기 큐빗을 유저 단말로 전송하고, 상기 큐빗을 상기 유저 단말로부터 루프백 받지 못한 경우 상기 큐빗이 정확한 기저에 의해 측정될 때의 측정 결과를 상기 유저 단말에 전송한다. 상기 유저 단말은 시큐리티 체크 모드가 아닐 때, 상기 큐빗 상에 시크릿 키를 인코딩하여 상기 시크릿 키가 인코딩된 상기 큐빗을 상기 서버로 루프백하고, 상기 시큐리티 체크 모드일 때, 상기 큐빗을 측정한다.

[0019] 본 발명의 일 실시예에 있어서, 상기 유저 단말이 저 전력 모드일 때 상기 서버가 상기 큐빗을 생성하고, 상기 유저 단말이 저 전력 모드가 아닐 때 상기 유저 단말이 상기 큐빗을 생성할 수 있다.

[0020] 본 발명의 일 실시예에 있어서, 상기 유저 단말은 상기 큐빗 상에 상기 시크릿 키를 인코딩할 때, I-gate 및 Pauli Y-gate를 이용할 수 있다. 상기 I-gate는 $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$일 수 있다. 상기 Pauli Y-gate는 $Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$일 수 있다.

[0021] 본 발명의 일 실시예에 있어서, 0을 인코딩하기 위해서 상기 유저 단말은 상기 I-gate를 이용할 수 있다. 1을 인코딩하기 위해서 상기 유저 단말은 상기 Pauli Y-gate를 이용할 수 있다.

[0022] 본 발명의 일 실시예에 있어서, 상기 큐빗은 광자(Photon)에 의해 전송될 수 있다. 상기 광자는 제1 및 제2 상태를 포함하고, 상기 광자는 제1 및 제2 기저(Basis)를 포함할 수 있다.

[0023] 본 발명의 일 실시예에 있어서, 상기 제1 상태는 0일 수 있다. 상기 제2 상태는 1일 수 있다. 상기 제1 기저는 수평 방향의 제1 축 및 수직 방향의 제2 축을 갖는 X 기저일 수 있다. 상기 제2 기저는 제1 대각 방향의 제3 축 및 상기 제1 대각 방향과 수직한 제2 대각 방향의 제4 축을 갖는 Z 기저일 수 있다.

[0024] 본 발명의 일 실시예에 있어서, 상기 큐빗은 전자(Electron)에 의해 전송될 수 있다. 상기 전자는 제1 및 제2 상태를 포함하고, 상기 전자는 제1 및 제2 기저를 포함할 수 있다.

[0025] 본 발명의 일 실시예에 있어서, 상기 양자 키 분배 방법은 상기 유저 단말이 측정한 상기 큐빗의 제1 측정 결과 및 상기 서버가 전송한 상기 큐빗이 정확한 기저에 의해 측정될 때의 제2 측정 결과를 기초로 상기 유저 단말이 큐빗 측정의 에러율을 계산하는 단계를 더 포함할 수 있다.

[0026] 본 발명의 일 실시예에 있어서, 상기 큐빗 측정의 상기 에러율이 기준 값보다 작으면 양자 키 분배가 계속 수행될 수 있다. 상기 큐빗 측정의 상기 에러율이 기준 값보다 크거가 같은 경우, 상기 양자 키 분배가 중단될 수 있다.

[0027] 본 발명의 일 실시예에 있어서, 상기 유저 단말은 상기 큐빗을 상기 서버로 루프백하는 복수의 미러를 포함할 수 있다.

발명의 효과

[0028] 상기와 같은 본 발명의 실시예들에 따른 저 전력 양자 키 분배 방법, 이를 이용한 양자 통신 방법 및 이를 수행

하는 양자 통신 시스템에서는, 상기 유저 단말이 저 전력 모드일 때, 상기 큐빗의 생성을 상기 서버가 담당하므로 상기 유저 단말의 큐빗 생성으로 인한 전력 부담을 감소시킬 수 있다.

[0029] 또한, 시큐리티 체크 시에도 상기 유저 단말은 최종적으로 에러가 검출된 경우에 한해서만 상기 서버로 그 에러 검출 결과를 전송하므로, 상기 유저 단말의 시큐리티 체크에 대한 전력 부담을 감소시킬 수 있다.

도면의 간단한 설명

[0030] 도 1은 본 발명의 일 실시예에 따른 양자 통신 시스템을 나타내는 개념도이다.

도 2는 시큐리티 체크 모드가 아닌 경우의 상기 양자 통신 시스템을 나타내는 개념도이다.

도 3은 종래의 양방향 프로토콜과 도 1의 양자 통신 시스템의 프로토콜의 클래시컬 비트의 교환을 나타내는 그래프이다.

도 4는 종래의 양방향 프로토콜과 도 1의 양자 통신 시스템의 프로토콜의 클래시컬 비트의 큐빗 측정을 나타내는 그래프이다.

도 5는 도 1의 양자 통신 시스템에 의해 수행되는 양자 키 분배 방법을 나타내는 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0031] 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.

[0032] 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.

[0033] 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.

[0034] 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.

[0035] 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.

[0036] 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.

[0037] 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.

[0038] 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.

[0039] 도 1은 본 발명의 일 실시예에 따른 양자 통신 시스템을 나타내는 개념도이다. 도 2는 시큐리티 체크 모드가 아닌 경우의 상기 양자 통신 시스템을 나타내는 개념도이다.

[0040] 도 1 내지 도 2를 참조하면, 상기 양자 통신 시스템은 서버(100) 및 유저 단말(200)을 포함한다.

[0041] 상기 서버(100)는 큐빗(QB)을 생성하여 상기 큐빗(QB)을 유저 단말(200)로 전송한다. 예를 들어, 상기 큐빗(QB)은 광자(Photon)에 의해 전송될 수 있다. 상기 광자는 제1 및 제2 상태를 포함하고, 상기 광자는 제1 및 제2 기저(Basis)를 포함할 수 있다. 상기 제1 상태는 0일 수 있다. 상기 제2 상태는 1일 수 있다. 상기 제1 기저는 수평 방향의 제1 축 및 수직 방향의 제2 축을 갖는 X 기저일 수 있다. 상기 제2 기저는 제1 대각 방향의 제3 축 및 상기 제1 대각 방향과 수직한 제2 대각 방향의 제4 축을 갖는 Z 기저일 수 있다.

[0042] 이와는 달리, 상기 큐빗은 전자(Electron)에 의해 전송될 수 있다. 상기 전자는 제1 및 제2 상태를 포함하고, 상기 전자는 제1 및 제2 기저를 포함할 수 있다.

[0043] 본 실시예는 상기 유저 단말(200)이 저 전력 모드에서 동작하는 경우를 예시한다. 상기 유저 단말(200)의 배터리 잔량이 충분한 경우에는 상기 유저 단말(200)이 저 전력 모드가 아닐 수 있다.

[0044] 예를 들어, 상기 유저 단말(200)이 저 전력 모드일 때 상기 서버(100)가 상기 큐빗을 생성하고, 상기 유저 단말(200)이 저 전력 모드가 아닐 때 상기 유저 단말(200)이 상기 큐빗을 생성할 수 있다

[0045] 상기 유저 단말(200)은 상기 큐빗(QB)을 상기 서버(100)로부터 수신한다. 상기 유저 단말(200)은 두 가지 동작 모드를 가질 수 있다. 상기 유저 단말(200)은 시큐리티 체크 모드 및 시큐리티 체크 모드가 아닌 일반 모드로 동작할 수 있다.

[0046] 상기 유저 단말은 상기 동작 모드가 시큐리티 체크 모드가 아닐 때, 상기 큐빗(QB) 상에 시크릿 키를 인코딩하여 상기 시크릿 키가 인코딩된 상기 큐빗(QB)을 상기 서버(100)로 루프백한다.

[0047] 상기 유저 단말(200)은 상기 큐빗(QB) 상에 상기 시크릿 키를 인코딩할 때, I-gate 및 Pauli Y-gate를 이용할 수 있다. 상기 I-gate는 $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ 일 수 있다. 상기 Pauli Y-gate는 $Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$ 일 수 있다.

[0048] 상기 유저 단말(200)은 0을 인코딩하기 위해서 상기 I-gate를 이용할 수 있다. 상기 유저 단말(200)은 1을 인코딩하기 위해서 상기 Pauli Y-gate를 이용할 수 있다.

[0049] 상기 유저 단말(200)은 랜덤 변수에 의해 상기 I-gate 및 상기 Pauli Y-gate를 적용할 수 있다. 예를 들어, 상기 유저 단말(200)은 상기 랜덤 변수가 0일 때, 상기 I-gate를 이용하여 상기 큐빗(QB) 상에 상기 시크릿 키를 인코딩하고, 상기 랜덤 변수가 1일 때, 상기 Pauli Y-gate를 이용하여 상기 큐빗(QB) 상에 상기 시크릿 키를 인코딩할 수 있다.

[0050] 도 2에서 보듯이, 예를 들어, 상기 유저 단말(200)은 I-gate 또는 Pauli Y-gate를 선택적으로 적용하는 인코딩부(I or Y) 및 상기 인코딩 후 상기 큐빗(QB)을 상기 서버(100)로 루프백하는 복수의 미러(M1, M2)를 포함할 수 있다. 예를 들어, 상기 유저 단말(200)은 상기 큐빗(QB)의 진행 방향과 45도 각도로 배치되는 제1 미러 및 상기 제1 미러와 수직으로 배치되는 제2 미러를 이용하여 상기 큐빗(QB)을 상기 서버(100)로 루프백할 수 있다.

[0051] 상기 유저 단말(200)은 상기 동작 모드가 시큐리티 체크 모드일 때, 상기 큐빗(QB)을 측정(measure)한다. 상기 큐빗(QB)의 측정은 비가역적인 작업이다. 따라서, 상기 큐빗(QB)이 한번 측정되면, 상기 큐빗(QB)의 측정 이전 상태로 되돌릴 수 없다.

[0052] 상기 유저 단말(200)은 시큐리티 체크를 위해 상기 큐빗(QB)의 측정 결과를 저장한다. 상기 유저 단말(200)이 상기 큐빗(QB)을 측정한 경우, 상기 큐빗(QB)은 상기 서버(100)로 루프백되지 않는다.

[0053] 상기 동작 모드가 상기 시큐리티 체크 모드가 아닌 경우에는 제1 시간(t1)에 상기 서버(100)로부터 상기 유저 단말(200)로 전송된 큐빗(QB)은 상기 제1 시간(t1)으로부터 상기 큐빗(QB)의 왕복 이동 시간(round trip time, RTT) 후인 제2 시간(t2)에 상기 서버(100)로 루프백된다.

[0054] 반면, 상기 동작 모드가 상기 시큐리티 체크 모드인 경우에는 상기 큐빗(QB)은 상기 유저 단말(200)에서 측정되고, 상기 서버(100)로 루프백되지 않으므로, 제3 시간(t3)에 상기 서버(100)로부터 상기 유저 단말(200)로 전송

된 큐빗(QB)은 상기 제3 시간(t3)으로부터 상기 큐빗(QB)의 왕복 이동 시간(round trip time, RTT) 후인 제4 시간(t4)에 상기 서버(100)로 루프백되지 않는다.

[0055] 상기 서버(100)가 상기 유저 단말(200)로부터 상기 큐빗(QB)을 루프백 받지 못한 경우, 상기 서버(100)가 상기 큐빗(QB)이 정확한 기저에 의해 측정될 때의 측정 결과를 상기 유저 단말(200)에 전송할 수 있다.

[0056] 예를 들어, 상기 서버(100)는 상기 제3 시간(t3)으로부터 상기 왕복 이동 시간 후인 상기 제4 시간(t4)에 상기 큐빗(QB)이 상기 서버(100)로 도착하지 않은 경우에 상기 큐빗(QB)이 정확한 기저에 의해 측정될 때의 측정 결과를 상기 유저 단말(200)에 전송할 수 있다.

[0057] 상기 서버(100)에 상기 전송한 큐빗(QB)이 돌아오지 않는 경우는 상기 큐빗(QB)이 전송 과정에서 길을 잃은 경우(lost)와 상기 유저 단말(200)에 의해 상기 큐빗(QB)이 측정된 경우가 있을 수 있다.

[0058] 상기 서버(100)는 상기 전송한 큐빗(QB)이 돌아오지 않은 경우, 상기 큐빗(QB)들의 위치 및 상기 큐빗(QB)들이 정확한 기저에 의해 측정될 때의 측정 결과를 상기 유저 단말(200)에 전송할 수 있다.

[0059] 상기 유저 단말(200)은 상기 유저 단말(200)이 상기 큐빗(QB)을 직접 측정한 제1 측정 결과 및 상기 서버(100)에 의해 전송된 정확한 기저에 의해 측정될 때의 제2 측정 결과를 비교하여 상기 큐빗 측정의 에러율을 계산한다.

[0060] 상기 큐빗 측정의 상기 에러율이 기준 값(ε)보다 작으면 상기 유저 단말(200) 및 상기 서버(100)는 양자 키 분배를 계속 수행한다. 반면, 상기 큐빗 측정의 상기 에러율이 기준 값(ε)보다 크거나 같으면 상기 유저 단말(200) 및 상기 서버(100)는 양자 키 분배를 중단할 수 있다.

[0061] 상기 에러율이 높다는 것은 상기 큐빗(QB)이 전송 과정에서 도청되고 있거나, 상기 통신의 신뢰성이 확보되지 않음을 의미할 수 있다.

[0062] 이와 같은 방식으로 상기 큐빗(QB)의 생성 및 루프백을 반복하면서 상기 서버(100) 및 상기 유저 단말(200)은 시크릿 키를 공유할 수 있다. 상기 유저 단말(200)이 상기 시크릿 키를 생성하고, 상기 시크릿 키를 상기 큐빗(QB)에 인코딩하여 상기 서버(100)로 루프백함으로 인해 상기 서버(100) 및 상기 유저 단말(200)은 양자 통신을 위한 시크릿 키를 공유하게 된다.

[0063] 상기 서버(100)와 유저 단말(200)은 상기 복수의 시크릿 키 비트들에 대한 정보 조정(information reconciliation) 및 비밀성 증폭(privacy amplification)을 수행하여, 보안 키(final key)를 공유할 수 있다. 상기와 같은 키 분배 동작 이후에, 양자 통신 시스템 내에서 상기 보안 키에 기초하여 데이터를 암호화하여 교환할 수 있다.

[0064] 상기 정보 조정은 상기 보안 키의 동일성을 확보하기 위한 동작일 수 있다. 구체적으로, 노이즈 및/또는 간섭 등에 의해 유저 단말(200)에서 전송된 상기 복수의 시크릿 키 비트들과, 상기 서버(100)에서 수신된 상기 복수의 시크릿 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.

[0065] 상기 비밀성 증폭은 상기 복수의 시크릿 키 비트들에서 제3자(third party)에게 누설된 정보를 제거하기 위한 동작일 수 있다. 구체적으로, 상기 비밀성 증폭은 상기 서버(100)와 상기 유저 단말(200)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 시크릿 키 비트들의 길이보다 감소될 수 있지만, 상기 보안 키의 랜덤성, 보안성, 안전성 및/또는 기밀성이 확보될 수 있다.

[0066] 상기와 같은 정보 조정 및 비밀성 증폭은 양자 후처리(post-process) 기술일 수 있으며, 상기 서버(100) 및 상기 유저 단말(200) 내부의 별도의 후처리부(미도시)에 의해 수행될 수 있다. 상기 정보 조정 및 상기 비밀성 증폭에 의해, 상기 서버(100)와 상기 유저 단말(200)이 실질적으로 동일한 상기 보안 키를 안전하게 공유할 수 있다.

[0067] 일 실시예에서, 상기 복수의 큐빗 그룹들 및 상기 복수의 리턴 큐빗 그룹들은, 상기 서버(100)와 상기 유저 단말(200) 사이의 양자 채널을 통해 전송될 수 있다. 상기 정보 조정 및 상기 비밀성 증폭은, 상기 서버(100)와 상기 유저 단말(200) 사이의 공개 채널을 통해 수행될 수 있다.

[0068] 상기 복수의 시크릿 키 비트들은 로우 키(raw key) 또는 선별 키(sifted key)라고 불릴 수 있고, 상기 보안 키

는 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.

[0069] 일 실시예에서, 상기 보안 키의 비트 수는 상기 복수의 시크릿 키 비트들의 수보다 적을 수 있다. 예를 들어, 상기 비밀성 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.

[0070] 도 3은 종래의 양방향 프로토콜과 도 1의 양자 통신 시스템의 프로토콜의 클래시컬 비트의 교환을 나타내는 그래프이다. 도 4는 종래의 양방향 프로토콜과 도 1의 양자 통신 시스템의 프로토콜의 클래시컬 비트의 큐빗 측정을 나타내는 그래프이다.

[0071] 도 3 및 도 4를 참조하면, 종래의 양방향 프로토콜에서는 상기 시큐리티 체크를 위해 상기 서버(100) 및 상기 유저 단말(200) 간의 클래시컬 비트의 교환이 계속하여 발생하므로, 상기 시크릿 키의 비트 수가 증가함에 따라 상기 클래시컬 비트의 교환의 횟수도 선형적으로 증가하였다. 예를 들어 종래의 양방향 프로토콜에서는 상기 유저 단말(200)이 상기 큐빗(QB)을 측정한 경우, 해당 측정의 결과에 오류가 있는지, 없는지를 매 측정시 마다 상기 서버(100)로 전송할 수 있다.

[0072] 반면, 본 프로토콜에서는 상기 시큐리티 체크를 위해 상기 유저 단말(200)이 상기 서버(100)에 보내는 메시지는 최종적으로 에러가 검출된 경우의 그 에러 검출 결과로 제한된다. 따라서, 상기 시크릿 키의 비트 수가 증가하더라도 상기 유저 단말(200)이 상기 서버(100)로 전송하는 클래시컬 비트 수가 증가하지 않고 일정하다.

[0073] 따라서, 본 실시예에서는 상기 유저 단말(200)이 상기 서버(100)로 클래시컬 비트를 전송하기 위한 전력 소모도 감소시킬 수 있다.

[0074] 시큐리티 체크 모드인 경우에, 상기 유저 단말(200)은 상기 서버(100)로부터 수신한 상기 큐빗(QB)을 측정한다. 상기 시큐리티 체크의 주기는 소비 전력 및 시큐리티 체크의 정확도 등을 고려하여 적절히 설정될 수 있다. 도 4에서는 열 개의 큐빗(QB) 중 하나의 큐빗(QB)에 대해 시큐리티 체크를 하는 경우를 예시하였다. 시큐리티 체크를 위해 상기 큐빗(QB)을 측정하는 주기 및 그 측정 기술에 대해서는 본 프로토콜과 종래의 양방향 프로토콜에 있어 특별한 차이점은 없다.

[0075] 도 5는 도 1의 양자 통신 시스템에 의해 수행되는 양자 키 분배 방법을 나타내는 흐름도이다.

[0076] 상기 양자 키 분배 방법에서 서버(100)가 큐빗(QB)을 생성하여 상기 큐빗(QB)을 유저 단말(200)로 전송한다 (단계 S100).

[0077] 상기 유저 단말(200)은 동작 모드가 시큐리티 체크 모드인지 아닌지 판단한다 (단계 S200).

[0078] 상기 동작 모드가 시큐리티 체크 모드가 아닐 때, 상기 유저 단말(200)은 상기 큐빗(QB) 상에 시크릿 키를 인코딩하여 상기 시크릿 키가 인코딩된 상기 큐빗(QB)을 상기 서버(100)로 루프백한다 (단계 S300).

[0079] 상기 동작 모드가 시큐리티 체크 모드일 때, 상기 유저 단말(200)은 상기 큐빗(QB)을 측정한다 (단계 S400).

[0080] 상기 서버(100)가 상기 큐빗(QB)을 루프백 받지 못한 경우, 상기 서버(100)는 상기 큐빗(QB)이 정확한 기저에 의해 측정될 때의 측정 결과를 상기 유저 단말(200)에 전송한다 (단계 S500).

[0081] 도 5에서, 상기 서버(100)가 상기 큐빗(QB)을 루프백 받지 못한 경우는 상기 유저 단말(200)이 상기 시큐리티 체크 모드인 경우로 예시하였으나, 이에 한정되지 않는다. 상기 큐빗(QB)이 통신 과정에서 길을 잃은 경우(lost)에도 상기 서버(100)는 상기 큐빗(QB)을 루프백 받지 못할 수 있다. 상기 서버(100)는 상기 큐빗(QB)이 상기 유저 단말(200)에 의해 측정된 것인지 상기 통신 과정에서 길을 잃은 것인지 구별할 수 없기 때문에, 상기 서버(100)는 상기 큐빗(QB)이 일정 기간(예컨대 RTT)동안 루프백되지 않으면, 상기 큐빗(QB)이 정확한 기저에 의해 측정될 때의 측정 결과를 상기 유저 단말(200)에 전송한다.

[0082] 상기 유저 단말(200)이 측정한 상기 큐빗의 제1 측정 결과 및 상기 서버(100)가 전송한 상기 큐빗이 정확한 기저에 의해 측정될 때의 제2 측정 결과를 기초로 상기 유저 단말(200)은 큐빗 측정의 에러율을 계산한다 (단계 S600).

[0083] 상기 유저 단말(200)은 상기 에러율을 기준 값(ε)과 비교한다 (단계 S700).

[0084] 상기 큐빗 측정의 상기 에러율이 기준 값(ε)보다 작으면 상기 유저 단말(200) 및 상기 서버(100)는 양자 키 분

배를 계속하여 수행한다 (단계 S800).

[0085] 반면, 상기 큐빗 측정의 상기 에러율이 기준 값(ε)보다 크거나 같으면 상기 유저 단말(200) 및 상기 서버(100)는 양자 키 분배를 중단할 수 있다 (단계 S900).

[0086] 본 실시예에 따르면, 상기 유저 단말(200)이 저 전력 모드일 때, 상기 큐빗(QB)의 생성을 상기 서버(100)가 담당하므로 상기 유저 단말(200)의 큐빗 생성으로 인한 전력 부담을 감소시킬 수 있다.

[0087] 또한, 시큐리티 체크 시에도 상기 유저 단말(200)은 최종적으로 에러가 검출된 경우에 한해서만 상기 서버(100)로 그 에러 검출 결과를 전송하므로, 상기 유저 단말(200)의 시큐리티 체크에 대한 전력 부담을 감소시킬 수 있다.

[0088] 본 발명의 실시예들에 따른 양자 통신에서의 저 전력 양자 키 분배 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 유저 단말은 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.

[0089] 본 발명의 실시예들에 따른 양자 통신에서의 양자 키 분배 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

[0090] 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.

[0091] 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

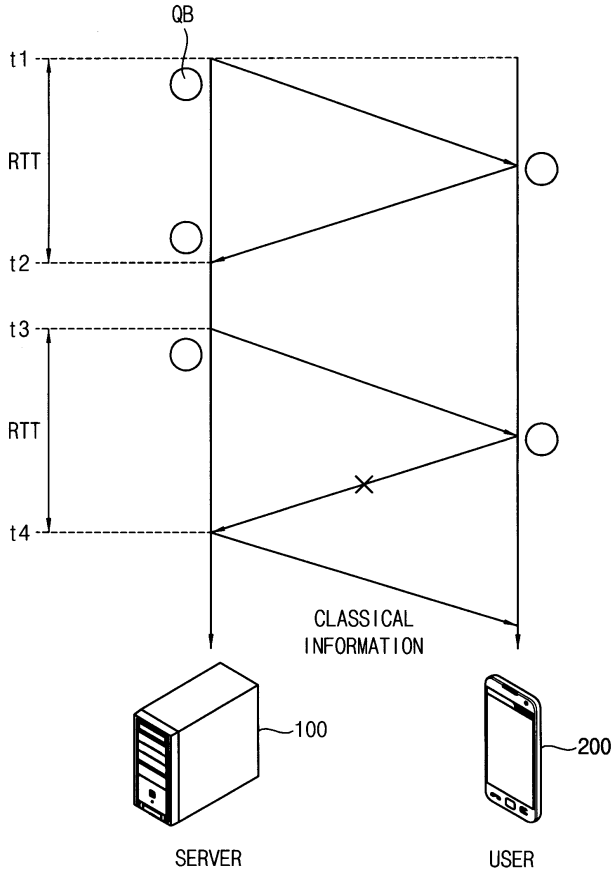
[0092] 100: 서버 200: 유저 단말

QB: 큐빗 M1: 제1 미러

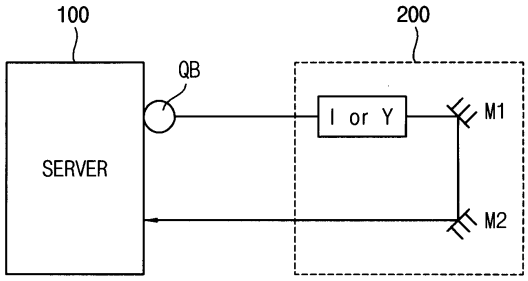
M2: 제2 미러

도면

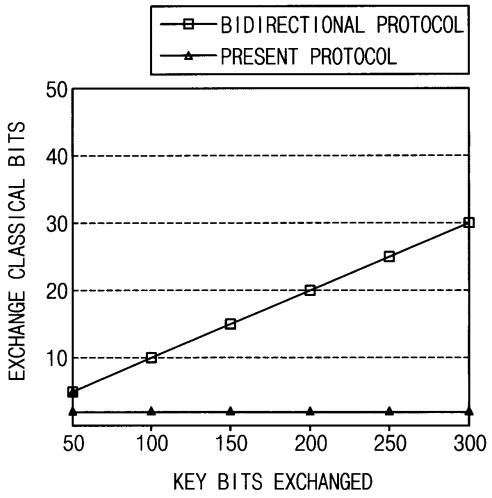
도면1


QB
t1
RTT
t2
t3
RTT
t4
CLASSICAL
INFORMATION
100
200
SERVER
USER

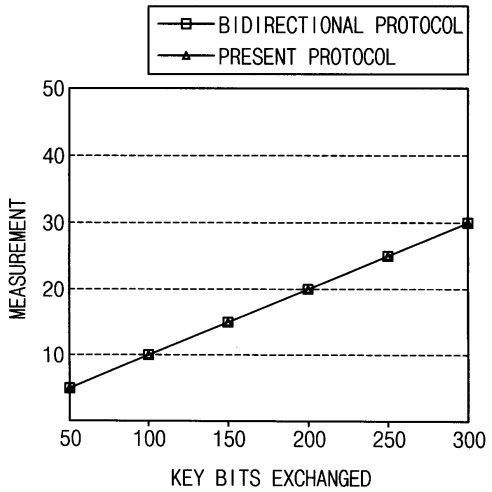
도면2


100
200
QB
SERVER
I or Y
M1
M2

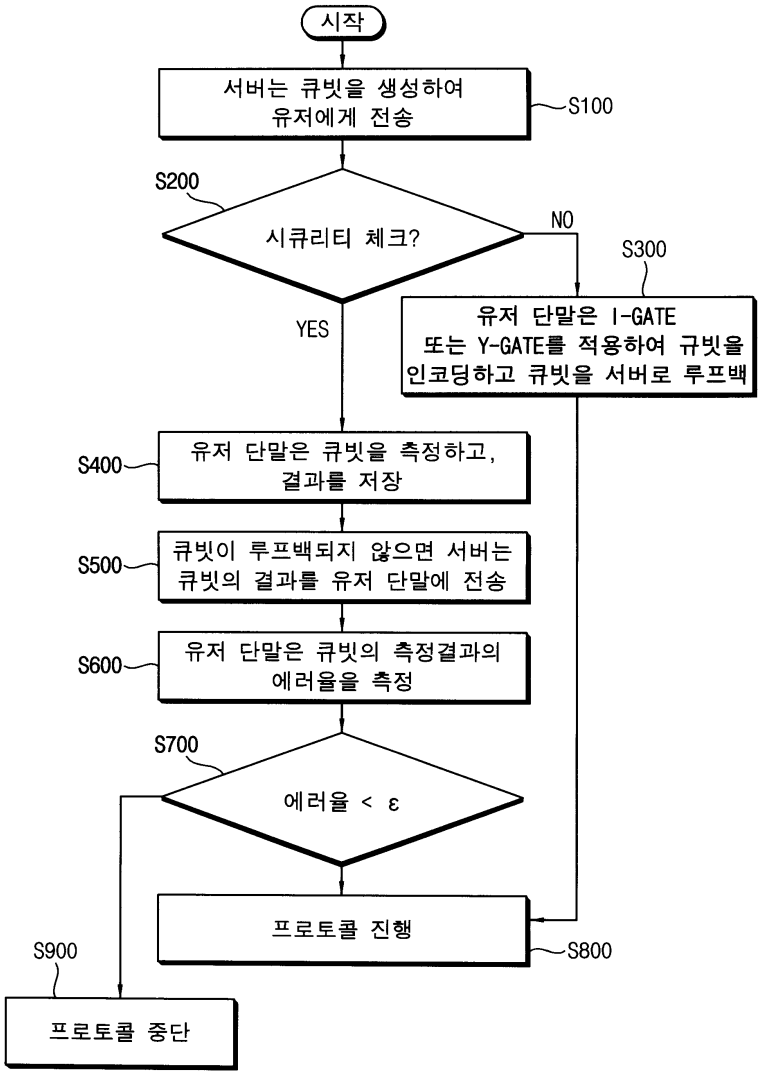
도면3


BIDIRECTIONAL PROTOCOL
PRESENT PROTOCOL
EXCHANGE CLASSICAL BITS
50
40
30
20
10
50
100
150
200
250
300
KEY BITS EXCHANGED

도면4


BIDIRECTIONAL PROTOCOL
PRESENT PROTOCOL
MEASUREMENT
50
40
30
20
10
50
100
150
200
250
300
KEY BITS EXCHANGED

도면5


시작
서버는 큐빗을 생성하여 유저에게 전송
S100
S200
시큐리티 체크?
NO
S300
YES
유저 단말은 I-GATE 또는 Y-GATE를 적용하여 규빗을 인코딩하고 큐빗을 서버로 루프백
S400
유저 단말은 큐빗을 측정하고, 결과를 저장
S500
큐빗이 루프백되지 않으면 서버는 큐빗의 결과를 유저 단말에 전송
S600
유저 단말은 큐빗의 측정결과의 에러율을 측정
S700
에러율 < ε
프로토콜 진행
S800
S900
프로토콜 중단