



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2024-0110291
(43) 공개일자 2024년07월15일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) H04B 10/70 (2013.01)
(52) CPC특허분류
H04L 9/0855 (2023.01)
H04B 10/70 (2013.01)
(21) 출원번호 10-2023-0002209
(22) 출원일자 2023년01월06일
심사청구일자 2023년01월06일

(71) 출원인
경희대학교 산학협력단
경기도 용인시 기흥구 덕영대로 1732 (서천동, 경희대학교 국제캠퍼스내)
(72) 발명자
신현동
경기도 수원시 영통구 청명로 132, 323동 501호(영통동, 벽산삼익아파트)
정해준
경기도 안양시 동안구 부림로 52, 505동 505호 (평촌동, 초원럭키아파트)
(뒷면에 계속)
(74) 대리인
김연권

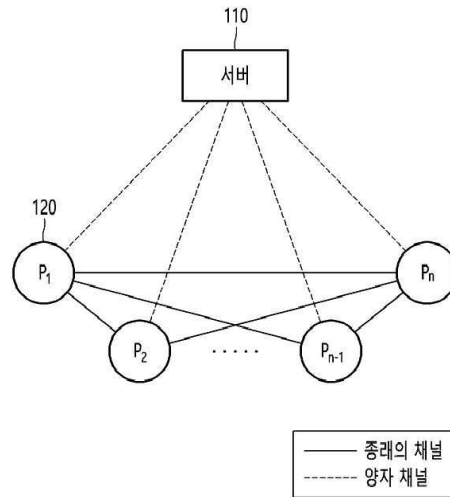
전체 청구항 수 : 총 13 항

(54) 발명의 명칭 보안 양자 정보 전송을 위한 방법 및 시스템

(57) 요약

본 개시의 기술적 사상에 의한 일 양태에 따르면, 제1 사용자 장치에 의해 실행되는 양자 통신 방법으로서, 얽힌(entangled) 벨 페어로부터 형성된 시퀀스를 서버로부터 수신하는 단계, 벨 기반 측정(Bell basis measurement)을 통해 수신한 시퀀스에 대해 얽힘 교환(entanglement swapping)을 수행하는 단계, 서버로부터 벨 페어의 초기 상태를 어나운스(announce)하도록 요청하고, 통신하고자 하는 제2 사용자 장치에 대응하는 δ 위치의 측정 결과를 요청하는 단계, 서버로부터 벨 페어의 초기 상태를 수신하고 제2 사용자 장치로부터 측정 결과를 수신하는 단계; 및 벨 페어의 초기 상태 및 측정 결과를 기초로 양자 채널의 보안을 확인하는 단계를 포함하는 양자 통신 방법이 개시된다.

대표도 - 도1



(72) 발명자

최민석

경기도 용인시 기흥구 서그대로53번길 3-7, 402호

여와이스 칸

경기도 용인시 기흥구 덕영대로 7321 경희대학교
국제캠퍼스 전자정보대학관 559호

난 패잉 싸

경기도 용인시 기흥구 덕영대로 7321 경희대학교
국제캠퍼스 전자정보대학관 559호

제이슨 윌리엄 쓰티아완

경기도 용인시 기흥구 덕영대로 7321 경희대학교
국제캠퍼스 전자정보대학관 559호

무하마드 탈하 라임

경기도 용인시 기흥구 덕영대로 7321 경희대학교
국제캠퍼스 전자정보대학관 559호

이 발명을 지원한 국가연구개발사업

과제고유번호	1711172939
과제번호	2022R1A4A3033401
부처명	과학기술정보통신부
과제관리(전문)기관명	한국연구재단
연구사업명	(혁신법) 기초연구실지원사업_개척형
연구과제명	[기초연구실_개척형] 무선-양자통신융합 기초연구실(1/3)
기 여 율	40/100
과제수행기관명	경희대학교 산학협력단
연구기간	2022.06.01 ~ 2025.02.28

이 발명을 지원한 국가연구개발사업

과제고유번호	1711155671
과제번호	2019R1A2C2007037
부처명	과학기술정보통신부
과제관리(전문)기관명	한국연구재단
연구사업명	(혁신법)이공분야기초연구사업/중견연구자지원사업/(유형1-2)중견연구
연구과제명	[중견연구 유형1-2] 양자네트워크 핵심기술 연구(4/5)
기 여 율	40/100
과제수행기관명	경희대학교 산학협력단
연구기간	2019.03.01 ~ 2024.02.29

이 발명을 지원한 국가연구개발사업

과제고유번호	1711152558
과제번호	2021-0-02046-002
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	(혁신법)정보통신방송혁신인재양성_2022
연구과제명	[정부] 2022 ITRC 6H 차세대 이동통신 기술 개발 (1단계 2차년도)(2/8)
기 여 율	20/100
과제수행기관명	경희대학교 산학협력단
연구기간	2021.07.01 ~ 2028.12.31

명세서

청구범위

청구항 1

제1 사용자 장치에 의해 실행되는 양자 통신 방법으로서,

얽힌(entangled) 벨 페어로부터 형성된 시퀀스를 서버로부터 수신하는 단계;

벨 기반 측정(Bell basis measurement)을 통해 수신한 시퀀스에 대해 얽힘 교환(entanglement swapping)을 수행하는 단계;

상기 서버로부터 벨 페어의 초기 상태를 어나운스(announce)하도록 요청하고, 통신하고자 하는 제2 사용자 장치에 대응하는 δ 위치의 측정 결과를 요청하는 단계;

상기 서버로부터 상기 벨 페어의 초기 상태를 수신하고 상기 제2 사용자 장치로부터 상기 측정 결과를 수신하는 단계; 및

상기 벨 페어의 초기 상태 및 상기 측정 결과를 기초로 양자 채널의 보안을 확인하는 단계를 포함하는 양자 통신 방법.

청구항 2

제1 항에 있어서,

상기 양자 통신 방법은,

상기 양자 채널의 보안이 양호하다고 판단하면, 상기 양자 채널의 보안을 확인하기 위해 사용한 얽힌(entangled) 벨 페어를 제외한 나머지 큐비트를 이용하여 벨 상태를 재생산하는 단계;

상기 재생산된 벨 상태에 $Z^{p_j} \otimes X^{q_j} (Z^{r_j} \otimes X^{s_j})$ 를 적용하여 인코딩하고 벨 기반(bell basis)으로 인코딩된 벨 상태를 측정한 측정 결과를 상기 제2 사용자 장치에 송신하는 단계;

상기 서버에 초기 벨 상태를 선언하도록 요청하는 단계;

상기 서버로부터 상기 초기 벨 상태를 수신하는 단계; 및

상기 수신된 초기 벨 상태를 기초로 메시지를 디코딩하는 단계를 더 포함하는 양자 통신 방법.

청구항 3

제2 항에 있어서,

상기 초기 벨 상태를 기초로 메시지를 디코딩하는 단계는,

상기 초기 벨 상태를 기초로 얽힘 교환으로 인해 붕괴된 벨 상태를 확인하는 단계; 및

상기 측정 결과 및 상기 붕괴된 벨 상태를 이용하여 상기 메시지를 디코딩하는 단계를 더 포함하는,

양자 통신 방법.

청구항 4

제1 항에 있어서,

상기 서버와 상기 제1 사용자 장치 간의 통신 채널 및 상기 서버와 상기 제2 사용자 장치 간의 통신 채널은 양자 채널인, 양자 통신 방법.

청구항 5

제1 항에 있어서,

상기 제1 사용자 장치와 상기 제2 사용자 장치 간의 통신 채널은 디지털 통신 채널인, 양자 통신 방법.

청구항 6

서버에 의해 실행되는 양자 통신 방법으로서,

제1 사용자 장치 및 제2 사용자 장치 간의 통신하고자 하는 메시지의 길이를 이용하여 벨 페어를 생성하고 생성된 벨 페어를 기초로 시퀀스를 형성하는 단계;

상기 형성된 시퀀스를 상기 제1 사용자 장치 및 상기 제2 사용자 장치에 분배하는 단계;

상기 제1 사용자 장치로부터 상기 벨 페어의 초기 상태에 대한 요청을 수신하는 경우, 상기 제1 사용자 장치 및 상기 제2 사용자 장치에 상기 벨 페어의 초기 상태를 어나운스(announce)하는 단계; 및

상기 제1 사용자 장치로부터 초기 벨 상태의 요청을 수신하는 경우, 상기 제1 사용자 장치에 상기 초기 벨 상태를 어나운스하는 단계

를 포함하는 양자 통신 방법.

청구항 7

제6 항에 있어서,

상기 서버와 상기 제1 사용자 장치 간의 통신 채널 및 상기 서버와 상기 제2 사용자 장치 간의 통신 채널은 양자 채널인, 양자 통신 방법.

청구항 8

통신부; 및

하나 이상의 프로세서

를 포함하고,

상기 하나 이상의 프로세서는,

상기 통신부가 얽힌(entangled) 벨 페어로부터 형성된 시퀀스를 서버로부터 수신하도록 제어하고, 벨 기반 측정(Bell basis measurement)을 통해 수신한 시퀀스에 대해 얽힘 교환(entanglement swapping)을 수행하고, 상기 서버로부터 벨 페어의 초기 상태를 어나운스(announce)하도록 요청하고, 통신하고자 하는 제2 사용자 장치에 대응하는 8 위치의 측정 결과를 요청하고, 상기 통신부가 상기 서버로부터 상기 벨 페어의 초기 상태를 수신하도록 제어하고 상기 제2 사용자 장치로부터 상기 측정 결과를 수신하도록 제어하고, 상기 벨 페어의 초기 상태 및 상기 측정 결과를 기초로 양자 채널의 보안을 확인하는,

사용자 장치.

청구항 9

제8 항에 있어서,

상기 하나 이상의 프로세서는,

상기 양자 채널의 보안이 양호하다고 판단하면, 상기 양자 채널의 보안을 확인하기 위해 사용한 얽힌(entangled) 벨 페어를 제외한 나머지 큐비트를 이용하여 벨 상태를 재생산하고, 상기 재생산된 벨 상태에 $Z^{p_j} \otimes X^{q_j} (Z^{r_j} \otimes X^{s_j})$ 를 적용하여 인코딩하고 벨 기반(bell basis)으로 인코딩된 벨 상태를 측정하여 측정 결과를 상기 제2 사용자 장치에 송신하도록 상기 통신부를 제어하고, 상기 서버에 초기 벨 상태를 선언하도록 요청하고, 상기 서버로부터 상기 초기 벨 상태를 수신하도록 상기 통신부를 제어하고, 상기 수신된 초기 벨 상태를 기초로 메시지를 디코딩하는, 사용자 장치.

청구항 10

제9 항에 있어서,

상기 하나 이상의 프로세서는,

상기 초기 벨 상태를 기초로 얽힘 교환으로 인해 붕괴된 벨 상태를 확인하고, 상기 측정 결과 및 상기 붕괴된 벨 상태를 이용하여 상기 메시지를 디코딩하는, 사용자 장치.

청구항 11

제8 항에 있어서,

상기 서버와 상기 제1 사용자 장치 간의 통신 채널 및 상기 서버와 상기 제2 사용자 장치 간의 통신 채널은 양자 채널인, 사용자 장치.

청구항 12

제8 항에 있어서,

상기 제1 사용자 장치와 상기 제2 사용자 장치 간의 통신 채널은 디지털 통신 채널인, 사용자 장치.

청구항 13

서버, 제1 사용자 장치 및 제2 사용자 장치를 포함하는 양자 통신 시스템으로서,

상기 서버는

제1 사용자 장치 및 제2 사용자 장치 간의 통신하고자 하는 메시지의 길이를 이용하여 벨 페어를 생성하고 생성된 벨 페어를 기초로 시퀀스를 형성하고, 상기 형성된 시퀀스를 상기 제1 사용자 장치 및 상기 제2 사용자 장치에 분배하고, 상기 제1 사용자 장치로부터 상기 벨 페어의 초기 상태에 대한 요청을 수신하는 경우, 상기 제1 사용자 장치 및 상기 제2 사용자 장치에 상기 벨 페어의 초기 상태를 어나운스(announce)하고, 상기 제1 사용자 장치로부터 초기 벨 상태의 요청을 수신하는 경우, 상기 제1 사용자 장치에 상기 초기 벨 상태를 어나운스하고, 상기 제1 사용자 장치는,

얽힌(entangled) 벨 페어로부터 형성된 시퀀스를 서버로부터 수신하고, 벨 기반 측정(Bell basis measurement)을 통해 수신한 시퀀스에 대해 얽힘 교환(entanglement swapping)을 수행하고, 상기 서버로부터 벨 페어의 초

기 상태를 어나운스(announce)하도록 요청하고, 통신하고자 하는 제2 사용자 장치에 대응하는 8 위치의 측정 결과를 요청하고, 상기 서버로부터 상기 벨 페어의 초기 상태를 수신하고 상기 제2 사용자 장치로부터 상기 측정 결과를 수신하고, 상기 벨 페어의 초기 상태 및 상기 측정 결과를 기초로 양자 채널의 보안을 확인하는, 양자 통신 시스템.

발명의 설명

기술 분야

[0001] 본 개시(disclosure)의 기술적 사상은 보안 양자 정보 전송을 위한 방법 및 시스템에 관한 것으로서, 보다 구체적으로, 네트워크 기반 어플리케이션에서의 보안 양자 정보 전송을 위한 방법 및 시스템에 관한 것이다.

배경 기술

[0002] 양자 암호화(Quantum cryptography)는 기존의 암호화 방식에 비해 안전하게 정보를 전달하는 새로운 패러다임을 제시한다. 가장 주목할 만한 것 중 하나는 양자 키 분배(Quantum Key Distribution, QKD)로, 무제한 컴퓨팅 리소스를 가진 제3자가 존재하는 경우에도 두 당사자가 비밀 키에 안전하게 동의할 수 있도록 한다. 이는 가로채기 시도(intercept attempt)가 감지되도록 하는 측정 붕괴(measurement collapse)라는 속성 때문이다. 또 다른 중요한 속성은 얽힘(entanglement) 속성으로, 어떤 고전적 상관관계보다 더 강력한 상관관계를 제공한다. 이 두 속성이 결합되어 상관 관계 값을 여러 당사자에게 안전하게 배포할 수 있는 기능을 제공한다.

[0003] 양자 키 분배가 적용된 이후 양자 통신이 종래의 통신의 범위를 훨씬 넘어서는 무조건적인 보안을 제공할 수 있음이 밝혀졌다. 양자 기술의 급속한 발전으로 안전한 양자 통신은 이제 QKD-지원 사전 공유 키 통신(QKD-assisted preshared key communication)뿐만 아니라 양자 보안 직접 통신(quantum secure direct communication, QSDC)으로 알려진 사전 공유 키를 사용하지 않는 직접 통신을 통해서도 달성할 수 있다. QSDC는 도청자에게 정보가 누출되지 않도록 보장하면서 정보 흐름을 한 방향으로 허용한다. 지금까지 얽힌 광자 및 단일 광자 등을 기반으로 많은 QSDC 프로토콜이 구현되었다.

[0004] 그러나 대부분의 통신 시나리오는 해당 노드가 발신자와 수신자 역할을 모두 수행해야 하는 양방향 대화이다. 따라서 QSDC의 개념은 두 당사자 간의 정보 교환을 동시에 가능하게 하는 양자 대화로 확장되었다. 2004년 Nguyen에 의해 처음 제안되었지만, 이는 인터셉트-재전송 공격(intercept-and-resend attack)에 취약하다. 이후 보안 문제와 정보 유출 문제를 극복하기 위해 다양한 유형의 양자 대화가 제시되었다. 최근 제어된 형태의 양자 통신(controlled form of quantum communication)은 양자 정보의 보안에 큰 영향력을 미쳐 양자 네트워크 분야에서 큰 주목을 받고 있다.

발명의 내용

해결하려는 과제

[0005] 본 개시의 기술적 사상이 이루고자 하는 기술적 과제는, 서버가 통신을 제어함에도 사용자 장치 간에 교환되는 정보를 서버에 노출시키지 않는, 보안이 보장된 양자 통신 방법 및 시스템을 제공하는데 있다.

[0006] 본 개시의 기술적 사상에 따른 양자 통신 방법 및 그 시스템이 이루고자 하는 기술적 과제는 이상에서 언급한 과제로 제한되지 않으며, 언급되지 않은 또 다른 과제는 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0007] 상기과 같은 목적을 달성하기 위하여, 본 개시의 기술적 사상에 의한 일 양태(aspect)에 따르면, 제1 사용자 장치에 의해 실행되는 양자 통신 방법으로서, 얽힘(entangled) 벨 페어로부터 형성된 시퀀스를 서버로부터 수신하는 단계, 벨 기반 측정(Bell basis measurement)을 통해 수신한 시퀀스에 대해 얽힘 교환(entanglement swapping)을 수행하는 단계, 서버로부터 벨 페어의 초기 상태를 어나운스(announce)하도록 요청하고, 통신하고자 하는 제2 사용자 장치에 대응하는 8 위치의 측정 결과를 요청하는 단계, 서버로부터 벨 페어의 초기 상태를 수신하고 제2 사용자 장치로부터 측정 결과를 수신하는 단계, 및 벨 페어의 초기 상태 및 측정 결과를 기초로

양자 채널의 보안을 확인하는 단계를 포함하는 양자 통신 방법이 개시된다.

- [0008] 예시적인 실시예에 따르면, 양자 통신 방법은, 양자 채널의 보안이 양호하다고 판단하면, 양자 채널의 보안을 확인하기 위해 사용한 얽힌(entangled) 벨 페어를 제외한 나머지 큐비트를 이용하여 벨 상태를 재생산하는 단계, 재생산된 벨 상태에 $Z^{p_j} \otimes X^{q_j} (Z^{r_j} \otimes X^{s_j})$ 를 적용하여 인코딩하고 벨 기반(bell basis)으로 인코딩된 벨 상태를 측정하여 측정 결과를 제2 사용자 장치에 송신하는 단계, 서버에 초기 벨 상태를 선언하도록 요청하는 단계, 서버로부터 초기 벨 상태를 수신하는 단계, 및 수신된 초기 벨 상태를 기초로 메시지를 디코딩하는 단계를 더 포함할 수 있다.
- [0009] 예시적인 실시예에 따르면, 초기 벨 상태를 기초로 메시지를 디코딩하는 단계는, 초기 벨 상태를 기초로 얽힘 교환으로 인해 붕괴된 벨 상태를 확인하는 단계 및 측정 결과 및 붕괴된 벨 상태를 이용하여 메시지를 디코딩하는 단계를 더 포함할 수 있다.
- [0010] 예시적인 실시예에 따르면, 서버와 제1 사용자 장치 간의 통신 채널 및 서버와 제2 사용자 장치 간의 통신 채널은 양자 채널일 수 있다.
- [0011] 예시적인 실시예에 따르면, 제1 사용자 장치와 제2 사용자 장치 간의 통신 채널은 디지털 통신 채널일 수 있다.
- [0012] 본 개시의 기술적 사상에 의한 다른 양태에 따르면, 사용자 장치는 통신부 및 하나 이상의 프로세서를 포함하고, 하나 이상의 프로세서는, 통신부가 얽힌(entangled) 벨 페어로부터 형성된 시퀀스를 서버로부터 수신하도록 제어하고, 벨 기반 측정(Bell basis measurement)을 통해 수신한 시퀀스에 대해 얽힘 교환(entanglement swapping)을 수행하고, 서버로부터 벨 페어의 초기 상태를 어나운스(announce)하도록 요청하고, 통신하고자 하는 제2 사용자 장치에 대응하는 6 위치의 측정 결과를 요청하고, 통신부가 서버로부터 벨 페어의 초기 상태를 수신하도록 제어하고 제2 사용자 장치로부터 측정 결과를 수신하도록 제어하고, 벨 페어의 초기 상태 및 측정 결과를 기초로 양자 채널의 보안을 확인할 수 있다.
- [0013] 예시적인 실시예에 따르면, 하나 이상의 프로세서는, 양자 채널의 보안이 양호하다고 판단하면, 양자 채널의 보안을 확인하기 위해 사용한 얽힌(entangled) 벨 페어를 제외한 나머지 큐비트를 이용하여 벨 상태를 재생산하고, 재생산된 벨 상태에 $Z^{p_j} \otimes X^{q_j} (Z^{r_j} \otimes X^{s_j})$ 를 적용하여 인코딩하고 벨 기반(bell basis)으로 인코딩된 벨 상태를 측정하여 측정 결과를 제2 사용자 장치에 송신하도록 통신부를 제어하고, 서버에 초기 벨 상태를 선언하도록 요청하고, 서버로부터 초기 벨 상태를 수신하도록 통신부를 제어하고, 수신된 초기 벨 상태를 기초로 메시지를 디코딩할 수 있다.
- [0014] 예시적인 실시예에 따르면, 하나 이상의 프로세서는, 초기 벨 상태를 기초로 얽힘 교환으로 인해 붕괴된 벨 상태를 확인하고, 측정 결과 및 붕괴된 벨 상태를 이용하여 메시지를 디코딩할 수 있다.
- [0015] 예시적인 실시예에 따르면, 서버와 제1 사용자 장치 간의 통신 채널 및 서버와 제2 사용자 장치 간의 통신 채널은 양자 채널일 수 있다.
- [0016] 예시적인 실시예에 따르면, 제1 사용자 장치와 제2 사용자 장치 간의 통신 채널은 디지털 통신 채널일 수 있다.
- [0017] 본 개시의 기술적 사상에 의한 또 다른 양태에 따르면, 서버에 의해 실행되는 양자 통신 방법으로서, 제1 사용자 장치 및 제2 사용자 장치 간의 통신하고자 하는 메시지의 길이를 이용하여 벨 페어를 생성하고 생성된 벨 페어를 기초로 시퀀스를 형성하는 단계, 형성된 시퀀스를 제1 사용자 장치 및 제2 사용자 장치에 분배하는 단계, 제1 사용자 장치로부터 벨 페어의 초기 상태에 대한 요청을 수신하는 경우, 제1 사용자 장치 및 제2 사용자 장치에 벨 페어의 초기 상태를 어나운스(announce)하는 단계, 및 제1 사용자 장치로부터 초기 벨 상태의 요청을 수신하는 경우, 제1 사용자 장치에 초기 벨 상태를 어나운스하는 단계를 포함하는 양자 통신 방법이 개시된다.
- [0018] 예시적인 실시예에 따르면, 서버와 제1 사용자 장치 간의 통신 채널 및 서버와 제2 사용자 장치 간의 통신 채널은 양자 채널일 수 있다.
- [0019] 본 개시의 기술적 사상에 의한 또 다른 양태에 따르면, 서버, 제1 사용자 장치 및 제2 사용자 장치를 포함하는 양자 통신 시스템으로서, 서버는 제1 사용자 장치 및 제2 사용자 장치 간의 통신하고자 하는 메시지의 길이를 이용하여 벨 페어를 생성하고 생성된 벨 페어를 기초로 시퀀스를 형성하고, 형성된 시퀀스를 제1 사용자 장치 및 제2 사용자 장치에 분배하고, 제1 사용자 장치로부터 벨 페어의 초기 상태에 대한 요청을 수신하는 경우, 제1 사용자 장치 및 제2 사용자 장치에 벨 페어의 초기 상태를 어나운스(announce)하고, 제1 사용자 장치로부터

초기 벨 상태의 요청을 수신하는 경우, 제1 사용자 장치에 초기 벨 상태를 어나운스하고, 제1 사용자 장치는, 얽힌(entangled) 벨 페어로부터 형성된 시퀀스를 서버로부터 수신하고, 벨 기반 측정(Bell basis measurement)을 통해 수신한 시퀀스에 대해 얽힘 교환(entanglement swapping)을 수행하고, 서버로부터 벨 페어의 초기 상태를 어나운스(announce)하도록 요청하고, 통신하고자 하는 제2 사용자 장치에 대응하는 δ 위치의 측정 결과를 요청하고, 서버로부터 벨 페어의 초기 상태를 수신하고 제2 사용자 장치로부터 측정 결과를 수신하고, 벨 페어의 초기 상태 및 측정 결과를 기초로 양자 채널의 보안을 확인할 수 있다.

[0020] 예시적인 실시예에 따르면, 제1 사용자 장치는, 양자 채널의 보안이 양호하다고 판단하면, 양자 채널의 보안을 확인하기 위해 사용한 얽힌(entangled) 벨 페어를 제외한 나머지 큐비트를 이용하여 벨 상태를 재생산하고, 재생산된 벨 상태에 $Z^{p_j} \otimes X^{q_j} (Z^{r_j} \otimes X^{s_j})$ 를 적용하여 인코딩하고 벨 기반(bell basis)으로 인코딩된 벨 상태를 측정하여 측정 결과를 제2 사용자 장치에 송신하고, 서버에 초기 벨 상태를 선언하도록 요청하고, 서버로부터 초기 벨 상태를 수신하고, 수신된 초기 벨 상태를 기초로 메시지를 디코딩할 수 있다.

[0021] 예시적인 실시예에 따르면, 제1 사용자 장치는, 초기 벨 상태를 기초로 얽힘 교환으로 인해 붕괴된 벨 상태를 확인하고, 측정 결과 및 붕괴된 벨 상태를 이용하여 메시지를 디코딩할 수 있다.

[0022] 예시적인 실시예에 따르면, 서버와 제1 사용자 장치 간의 통신 채널 및 서버와 제2 사용자 장치 간의 통신 채널은 양자 채널일 수 있다.

[0023] 예시적인 실시예에 따르면, 제1 사용자 장치와 제2 사용자 장치 간의 통신 채널은 디지털 통신 채널일 수 있다.

[0024] 본 개시의 기술적 사상에 의한 또 다른 양태에 따르면, 하드웨어와 결합되어 전술한 방법을 실행시키기 위하여 컴퓨터 판독 가능한 기록매체에 저장된 컴퓨터 프로그램이 개시된다.

[0025] 본 개시의 기술적 사상에 의한 또 다른 양태에 따르면, 하드웨어와 결합되어 전술한 방법을 실행시키기 위하여 컴퓨터 프로그램이 저장된 컴퓨터 판독 가능한 기록매체가 개시된다.

발명의 효과

[0026] 본 개시의 기술적 사상에 따른 양자 통신 방법 및 시스템에 따르면, 네트워크 상에 있는 복수의 참가자가 동시에 안전하게 정보를 교환할 수 있는 네트워크를 구현할 수 있다.

[0027] 나아가, 본 개시의 기술적 사상에 따른 양자 통신 방법 및 시스템에 따르면, 서버가 통신을 제어함에도 사용자 장치 간에 교환되는 정보를 서버에 노출시키지 않으면서 통신할 수 있도록 한다.

[0028] 본 개시의 기술적 사상에 따른 양자 통신 방법 및 시스템이 얻을 수 있는 효과는 이상에서 언급한 효과들로 제한되지 않으며, 언급하지 않은 또 다른 효과들은 아래의 기재로부터 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[0029] 본 개시에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 간단한 설명이 제공된다.

도 1은 본 개시의 일 실시예에 따른 양자 통신 시스템의 구성을 도시한다.

도 2 및 도 3은 본 개시의 일 실시예에 따른 양자 통신 방법의 흐름도이다.

도 4는 본 개시의 일 실시예에 따라 얽힘 교환 후 붕괴된(Collapsed) 벨 상태를 나타낸다.

도 5는 본 개시의 일 실시예에 따른 변형된 프로토콜의 성능을 비교하는 그래프이다.

도 6은 본 개시의 일 실시예에 따른 에러 확률이 증가함에 따른 목록 상관 에러의 경향을 나타내는 그래프이다.

발명을 실시하기 위한 구체적인 내용

[0030] 본 개시의 기술적 사상에 따른 예시적인 실시예들은 당해 기술 분야에서 통상의 지식을 가진 자에게 본 개시의 기술적 사상을 더욱 완전하게 설명하기 위하여 제공되는 것으로, 아래의 실시예들은 여러 가지 다른 형태로 변형될 수 있으며, 본 개시의 기술적 사상의 범위가 아래의 실시예들로 한정되는 것은 아니다. 오히려, 이들 실시예들은 본 개시를 더욱 충실하고 완전하게 하며 당업자에게 본 발명의 기술적 사상을 완전하게 전달하기 위하여 제공되는 것이다.

- [0031] 본 개시에서 제1, 제2 등의 용어가 다양한 부재, 영역, 층들, 부위 및/또는 구성 요소들을 설명하기 위하여 사용되지만, 이들 부재, 부품, 영역, 층들, 부위 및/또는 구성 요소들은 이들 용어에 의해 한정되어서는 안 됨은 자명하다. 이들 용어는 특정 순서나 상하, 또는 우열을 의미하지 않으며, 하나의 부재, 영역, 부위, 또는 구성 요소를 다른 부재, 영역, 부위 또는 구성 요소와 구별하기 위하여만 사용된다. 따라서, 이하 상술할 제1 부재, 영역, 부위 또는 구성 요소는 본 개시의 기술적 사상의 가르침으로부터 벗어나지 않고서도 제2 부재, 영역, 부위 또는 구성 요소를 지칭할 수 있다. 예를 들면, 본 개시의 권리 범위로부터 이탈되지 않은 채 제1 구성 요소는 제2 구성 요소로 명명될 수 있고, 유사하게 제2 구성 요소도 제1 구성 요소로 명명될 수 있다.
- [0032] 달리 정의되지 않는 한, 여기에 사용되는 모든 용어들은 기술 용어와 과학 용어를 포함하여 본 개시의 개념이 속하는 기술 분야에서 통상의 지식을 가진 자가 공통적으로 이해하고 있는 바와 동일한 의미를 지닌다. 또한, 통상적으로 사용되는, 사전에 정의된 바와 같은 용어들은 관련되는 기술의 맥락에서 이들이 의미하는 바와 일관되는 의미를 갖는 것으로 해석되어야 하며, 여기에 명시적으로 정의하지 않는 한 과도하게 형식적인 의미로 해석되어서는 아니 될 것이다.
- [0033] 어떤 실시예가 달리 구현 가능한 경우에 특정한 공정 순서는 설명되는 순서와 다르게 수행될 수도 있다. 예를 들면, 연속하여 설명되는 두 공정이 실질적으로 동시에 수행될 수도 있고, 설명되는 순서와 반대의 순서로 수행될 수도 있다.
- [0034] 첨부한 도면에 있어서, 예를 들면, 제조 기술 및/또는 공차에 따라, 도시된 형상의 변형들이 예상될 수 있다. 따라서, 본 개시의 기술적 사상에 의한 실시예들은 본 개시에 도시된 영역의 특정 형상에 제한된 것으로 해석되어서는 아니 되며, 예를 들면, 제조 과정에서 초래되는 형상의 변화를 포함하여야 한다. 도면 상의 동일한 구성 요소에 대해서는 동일한 참조부호를 사용하고, 이들에 대한 중복된 설명은 생략한다.
- [0035] 여기에서 사용된 '및/또는' 용어는 언급된 부재들의 각각 및 하나 이상의 모든 조합을 포함한다.
- [0036] 이하에서는 첨부한 도면들을 참조하여 본 개시의 기술적 사상에 의한 실시예들에 대해 상세히 설명한다.
- [0038] 도 1은 본 개시의 일 실시예에 따른 양자 통신 시스템의 구성을 도시한다. 도 1을 참조하면, 양자 통신 시스템은 서버(110) 및 복수의 사용자 장치(120)를 포함한다.
- [0039] 본 개시에서는 큐비트를 반송하는 메시지가 양자 채널을 통과하지 않는 네트워크를 위한 제어된 양자 대화 프로토콜을 제공한다. 본 개시의 방법에 따르면 서버가 제공하는 양자 자원을 확인하고, 서버가 통신을 통제하더라도 서버에 비밀 메시지의 일부를 공개하지 않는 교환 메시지의 보안을 보장할 수 있다. 본 개시를 통해 제시되는 이와 같은 방식은 모든 종류의 네트워크 통신 시나리오에서 사용할 수 있다.
- [0040] 정보 보안 위협이 증가함에 따라 네트워크 내 참여자 간에 정보가 안전하게 전송되도록 하는 것이 최우선 순위이다. 이러한 요구 사항을 충족하기 위해 본 개시는 네트워크에서 사용할 수 있는 새로운 제어 양자 대화 프로토콜을 제시한다. 제어 양자 대화의 원칙은 컨트롤러가 통신에 동의하는 경우에만 참가자가 동시에 정보를 교환할 수 있다는 것이다. 이 체계에서 서버는 엄밀 교환을 통해 네트워크 내에서 양자 대화를 수행하려는 두 참가자에게 양자 자원을 지원한다. 신뢰할 수 있는 메시지 전송을 달성하기 위해 참가자는 서버에서 보낸 양자 리소스가 자신을 제외한 사람에게 알려지지 않도록 해야 하며, 큐비트를 운반하는 메시지는 양자 채널을 통과하지 않으며 서버가 통신의 컨트롤러인 경우에도 서버가 비밀 메시지의 일부를 알도록 허용해서는 안 된다.
- [0041] 도 1과 같은 네트워크에서 $i = \{1, 2, \dots, N\}$ 인 N 개의 사용자 장치 P_i 와 사용자 장치 간의 통신을 제어하는 서버가 존재할 수 있다. 양자 채널은 서버와 각 사용자 장치 사이에만 존재하며 사용자 장치 사이에는 양자 통신 채널이 없다. 상대방과 통신을 하고자 하는 사용자 장치는 이를 서버에 알리고, 상대방 사용자 장치의 ID를 알려주고, 메시지의 최대 길이를 알려주어야 한다. 편의상 도 1의 사용자 장치 P_1 (제1 사용자 장치)이 사용자 장치 P_N (제2 사용자 장치)과 정보 교환을 원하고 이를 서버에 알린다고 가정하여, 양자 대화 작업을 수행하기 위해 수행할 단계들 도 2 및 도 3을 참조하며 아래에서 설명한다.
- [0042] 1단계: 상태 준비
- [0043] 서버는 $|X_j\rangle_{AB}$ 및 $|X_{m+j}\rangle_{CD}$ 와 같이 $2(m+\delta)$ Bell 상태를 생성한다. 여기서 $j = \{1, 2, \dots, m\}$ 이고 $2m$ 은 사용자 장치 간에 교환하고자 하는 비밀 메시지의 길이이다. 여기서 벨 상태는

$|\chi_j\rangle_{AB}, |\chi_{m+j}\rangle_{CD} \in \{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$ 이며,

$$|\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00 \pm 11\rangle), \quad |\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01 \pm 10\rangle).$$

[0044]

[0045]

이다.

[0046]

서버는 얽힌 쌍의 큐비트로부터 S_A, S_B, S_C, S_D 시퀀스를 형성한다. 여기서 S_A 는 $|\chi_j\rangle_{AB}$ 의 A 입자에 해당하고 다른 시퀀스에도 동일하게 적용된다. 그 후, 서버는 시퀀스 S_A 및 S_C 를 P_1 에 배포하고 시퀀스 S_B 및 S_D 를 P_N 에 배포한다.

[0047]

2단계: 얽힘 교환(Entanglement Swapping)

[0048]

P_1 과 P_N 이 해당 시퀀스를 수신하면 P_1 은 S_A 와 S_C 의 큐비트에 대해 벨 기반 측정(Bell basis measurement)을 수행하고 P_N 은 S_B 와 S_D 의 큐비트에 대해 벨 기반 측정을 수행한다.

[0049]

3단계: 보안 확인

[0050]

양자 채널의 보안을 보장하기 위해 P_1 은 서버에 2δ 벨 쌍의 초기 상태를 공개적으로 알리도록(announce) 요청하고, P_N 에 해당 δ 위치의 측정 결과를 알려주도록 요청한다. 이러한 정보를 바탕으로 P_1 은 양자 채널에 도청자가 있는지 여부를 확인할 수 있다. P_1 이 양자 채널이 안전하다고 결론을 내리면 4단계로 이동한다.

[0051]

4단계: 벨 상태 재생산(reproducing)

[0052]

보안 확인을 위해 사용된 2δ 얽힌 쌍을 제외하고 P_1 과 P_N 은 측정 결과를 기반으로 나머지 $2m$ 벨 상태를 재생산한다.

[0053]

5단계: 메시지 인코딩

[0054]

비밀 메시지를 인코딩하기 위해 $P_1(P_N)$ 은 재생산된 벨 상태에 $Z^{p_j}X^{q_j}(Z^{r_j}X^{s_j})$ 를 적용한다. 사용자 장치들은 또한 프로토콜을 시작하기 전에 벨 상태와 고전 메시지(classic message) 간의 번역에 동의한다. 벨 상태 $\{|\phi^+\rangle, |\psi^+\rangle, |\phi^-\rangle, |\psi^-\rangle\}$ 는 고전 메시지 $\{00, 01, 10, 11\}$ 로 변환된다. 여기서 고전 메시지는 종래의 컴퓨팅을 이용하는 메시지를 지시한다.

[0055]

6단계: 권한 부여

[0056]

P_1 및 P_N 은 다시 벨 기준(Bell basis)으로 인코딩된 벨 상태를 측정하고 공개(public) 고전(종래의) 채널을 통해 결과를 $x_{j1}x_{j2}$ 및 $x_{j3}x_{j4}$ 로 알린다. 여전히 사용자 장치는 초기 벨 상태에 대한 정보가 없기 때문에 서로의 메시지를 해독할 수 없다. 따라서 사용자 장치는 서버에 초기 상태를 선언하도록 요청한다.

[0057]

7단계: 메시지 디코딩

[0058]

서버의 허가, 즉 초기 벨 상태 발표(announcement) 시 사용자 장치는 도 4의 표와 같이 얽힘 교환 작업 후 붕괴된 벨 상태가 무엇인지 즉시 알 수 있다.

$$\begin{aligned}
 A_0 &\rightarrow \{|\phi_{AC}^+\rangle|\phi_{BD}^+\rangle, |\phi_{AC}^-\rangle|\phi_{BD}^-\rangle, \\
 &\quad |\psi_{AC}^+\rangle|\psi_{BD}^+\rangle, |\psi_{AC}^-\rangle|\psi_{BD}^-\rangle\} \\
 A_1 &\rightarrow \{|\phi_{AC}^-\rangle|\phi_{BD}^+\rangle, |\phi_{AC}^+\rangle|\phi_{BD}^-\rangle, \\
 &\quad |\psi_{AC}^+\rangle|\psi_{BD}^-\rangle, |\psi_{AC}^-\rangle|\psi_{BD}^+\rangle\} \\
 A_2 &\rightarrow \{|\phi_{AC}^+\rangle|\psi_{BD}^+\rangle, |\phi_{AC}^-\rangle|\psi_{BD}^-\rangle, \\
 &\quad |\psi_{AC}^+\rangle|\phi_{BD}^+\rangle, |\psi_{AC}^-\rangle|\phi_{BD}^-\rangle\} \\
 A_3 &\rightarrow \{|\phi_{AC}^-\rangle|\psi_{BD}^+\rangle, |\phi_{AC}^+\rangle|\psi_{BD}^-\rangle, \\
 &\quad |\psi_{AC}^-\rangle|\phi_{BD}^+\rangle, |\psi_{AC}^+\rangle|\phi_{BD}^-\rangle\}
 \end{aligned}$$

[0059]

[0060] P_1 및 P_N 의 붕괴된 벨 상태를 고전 메시지 형식으로 각각 $y_{j1}y_{j2}$ 와 $y_{j3}y_{j4}$ 으로 표시할 수 있다. 마지막으로 서로의 비밀 메시지를 다음과 같이 디코딩할 수 있다.

$$\begin{aligned}
 p_j q_j &= x_{j1}x_{j2} \oplus y_{j1}y_{j2} \\
 r_j s_j &= x_{j3}x_{j4} \oplus y_{j3}y_{j4}
 \end{aligned}$$

[0061]

[0062] 모든 양자 통신의 중요한 문제는 보안이다. 얽힘 교환의 고유한 속성으로 인해 서버는 사용자 장치에서 붕괴된 벨 상태를 알 수 없다. 두 쌍이 모두 동일한 확률로 가능한 4개의 쌍 세트에 붕괴되기 때문이다. 정보를 교환하는 동안 정보를 운반하는 입자는 양자 채널을 통과하지 않는다. 또한 서버는 사용자 장치의 고전적인 어나운스먼트(classical announcement)에서 비밀 메시지를 추출할 수 없다. 따라서 제안된 프로토콜은 두 참가자 간의 안전한 정보 교환을 보장한다. 본 개시의 양자 통신 방법은 군사, 금융, 의료 등 모든 종류의 네트워크 통신 시나리오에서 사용할 수 있다.

[0063]

본 개시의 양자 통신 방법이 제1 사용자 장치에 의해 실행되는 것을 기준으로 다시 설명하면, 제1 사용자 장치에 의해 실행되는 양자 통신 방법은, 얽힌(entangled) 벨 페어로부터 형성된 시퀀스를 서버로부터 수신하는 단계, 벨 기반 측정(Bell basis measurement)을 통해 수신한 시퀀스에 대해 얽힘 교환(entanglement swapping)을 수행하는 단계, 서버로부터 벨 페어의 초기 상태를 어나운스(announce)하도록 요청하고, 통신하고자 하는 제2 사용자 장치에 대응하는 δ 위치의 측정 결과를 요청하는 단계, 서버로부터 벨 페어의 초기 상태를 수신하고 제2 사용자 장치로부터 측정 결과를 수신하는 단계, 및 벨 페어의 초기 상태 및 측정 결과를 기초로 양자 채널의 보안을 확인하는 단계를 포함할 수 있다.

[0064]

일 실시예에 따르면, 제1 사용자 장치는, 양자 채널의 보안이 양호하다고 판단하면, 양자 채널의 보안을 확인하기 위해 사용한 얽힌(entangled) 벨 페어를 제외한 나머지 큐비트를 이용하여 벨 상태를 재생산하고, 재생산된 벨 상태에 $Z^{p_j} \otimes X^{q_j} (Z^{r_j} \otimes X^{s_j})$ 를 적용하여 인코딩하고 벨 기반(bell basis)으로 인코딩된 벨 상태를 측정하는 측정 결과를 제2 사용자 장치에 송신할 수 있다. 그리고 서버에 초기 벨 상태를 선언하도록 요청하여 서버로부터 초기 벨 상태를 수신하고, 수신된 초기 벨 상태를 기초로 메시지를 디코딩할 수 있다.

[0065]

일 실시예에 따르면, 제1 사용자 장치가 초기 벨 상태를 기초로 메시지를 디코딩하는 경우, 제1 사용자 장치는 초기 벨 상태를 기초로 얽힘 교환으로 인해 붕괴된 벨 상태를 확인하고, 측정 결과 및 붕괴된 벨 상태를 이용하여 메시지를 디코딩할 수 있다.

[0066]

일 실시예에 따르면, 도 1에 도시된 바와 같이, 서버와 제1 사용자 장치 간의 통신 채널 및 서버와 제2 사용자 장치 간의 통신 채널은 양자 채널일 수 있다. 또한, 제1 사용자 장치와 제2 사용자 장치 간의 통신 채널은 양자 채널이 아닌 종래의 통신 채널, 즉, 디지털 통신 채널일 수 있다.

[0067] 한편, 원격 의료(Telehealth)는 환자의 건강 상태를 개선하기 위해 통신 인프라를 통해 한 위치에서 다른 위치로 의료 정보를 교환하는 것을 의미한다. 건강 관련 정보는 민감한 정보이므로 이 정보를 안전하게 전송하는 것이 중요하다. 본 개시는 양자 보안 원격의료 시스템을 위한 프로토콜을 제공한다. 본 개시에서 제공되는 프로토콜은 다양한 종류의 공격에도 강인하다. 따라서, 이 프로토콜을 사용하면 서버, 즉, 서비스 제공 네트워크(SN)를 통해 환자와 의사 간에 의료 정보를 안전하게 교환할 수 있다.

[0068] 본 개시에서 제공되는 프로토콜은 보안이 필요한 정보, 예컨대, 의료 정보의 양방향 교환을 위해 서비스 제공 네트워크(SN)의 도움으로 양 측의 사용자 단말 사이의 보안 연결을 설정할 수 있다. 나아가, 이러한 프로토콜은 외부의 적과 악의적인 SN에 대해 강인하다.

[0069] 양자 통신 시스템은 로컬 작업 및 클래식 통신(local operation and classical communication, LOCC)을 수행할 수 있는 서버, 즉, 서비스 제공 네트워크(Service Providing Network), 제1 사용자 단말 및 제2 사용자 단말을 포함할 수 있다. 도 1에 도시된 바와 같이, 제1 사용자 단말과 서버, 제2 사용자 단말과 서버는 양자 채널을 통해, 제1 사용자 단말과 제2 사용자 단말은 클래식 인증 채널을 통해 연결될 수 있다. 여기서 클래식 인증 채널은 양자 채널이 아닌 종래의 통신 방식을 사용하는 채널을 의미한다.

[0070] SN은 오작동이 허용되지만 인코딩된 데이터를 변조할 수 없으며 보안 통신을 위한 양자 리소스를 제공하는 제3자이다. 서버는 네트워크의 양자 채널을 통해 GHZ 상태

$$|GHZ\rangle = \frac{1}{\sqrt{2}} (|0_S 0_A 0_B\rangle + |1_S 1_A 1_B\rangle)$$

[0071]

[0072] 를 생성하고 배포한다. 제1 사용자 단말과 제2 사용자 단말은 공유 상태를 검증하기 위해 공동 작업을 한다. 검증(verification) 후 보안 연결이 설정된다. 네트워크의 모든 당사자는 아다마르 베이스(Hadamard basis)로 양자 상태를 측정한다. 그 후, 제1 사용자 단말과 제2 사용자 단말은 간단한 XOR 연산으로 측정된 상태를 인코딩하여 보안이 필요한 정보를 교환한다.

[0073] 구체적으로, 본 개시의 양자 통신 시스템에 대해 자세히 설명한다.

[0074] 1) SN은 전술한 바와 같이 n 개의 GHZ 상태를 생성하고 모든 큐비트를 GS, GA 및 GB의 세 개의 시퀀스로 정렬한다. 여기서 GS, GA 및 GB는 각각 n 순서 GHZ 상태의 S, A 및 B 광자로 구성된다.

[0075] 2) SN은 시퀀스 GA와 GB를 각각 제1 사용자 장치 및 제2 사용자 장치에 송신하고, 시퀀스 GS를 보유한다.

[0076] 3) 제1 사용자 장치는 Z 기준(basis) $\{|0\rangle, |1\rangle\}$ 또는 X 기준(basis) $\{|+\rangle, |-\rangle\}$ 과 n 개의 GHZ 상태의 하위 집합 m 을 무작위로 선택하여 검증 절차를 수행한다. 제1 사용자 장치는 이러한 GHZ 상태의 각 측정에 대한 기반(basis)과 위치를 통지(announce)한다.

[0077] 4) 각 당사자는 통지된 기준에 따라 측정한다. 먼저 SN은 클래식 인증 채널을 통해 제1 사용자 단말에게 측정 결과를 통지한다. 그 후, 제2 사용자 단말이 측정 결과를 알린다. 제1 사용자 단말은 결과를 비교하여 에러 레이트를 분석한다. 에러 레이트가 임계치를 초과하는 경우, 프로토콜을 중단한다. 그렇지 않다면 통신은 계속된다.

[0078] 5) 그 후, 검증을 위해 사용된 GHZ 상태의 큐비트를 폐기한다. 각 당사자는 X 기준(basis)으로 큐비트를 측정한다.

[0079] 6) 제1 사용자 단말과 제2 사용자 단말은 측정 결과에 대한 정보를 단순히 XOR 연산으로 인코딩합니다. 예를 들어 제1 사용자 단말이 제2 사용자 단말에게 0을 송신하고 측정 결과가 1이라면 인코딩된 데이터는 $0 \oplus 1 = 1$ 이다.

[0080] 7) SN이 먼저 측정 결과를 통지(announce)한다. 그런 다음 제1 사용자 단말과 제2 사용자 단말은 인코딩된 정보를 통지한다.

[0081] 8) 제1 사용자 단말과 제2 사용자 단말은 비밀 메시지를 얻을 수 있다. 제1 사용자 단말 및 제2 사용자 단말 모두 세 종류의 비트, 즉 SN의 게시 비트(publish bits), 상대방의 게시 비트 및 자체 측정 비트를 가지고 있다. 이 세 비트를 단순히 XOR하여 결과를 얻을 수 있다.

- [0082] 일 예시로, 서비스 제공 네트워크(SN)가 GHZ 상태의 생성 및 배포 중에 프로토콜을 공격하는 경우, SN은 프라이빗 데이터를 캡처하기 위해 거짓 GHZ 상태를 준비하고 당사자 간에 배포하여 공격을 수행할 수 있다. 따라서 이 시간 동안 악의적인 SN이 공격할 더 좋은 기회이다.
- [0083] 다른 예시로, 외부의 적이 GHZ 상태 전송 중에 프로토콜을 공격하는 경우, 즉, SN에서 제1 사용자 장치 또는 제2 사용자 장치로 GHZ 상태를 전송하는 동안 공격이 수행되는 경우, 프로토콜의 전체 프로세스 동안 한 번만 시퀀스로서 GA와 GB가 양자 채널을 통해 전송된다. 이는 외부의 공격자가 사적인 정보를 얻기 위해 능동적인 공격(예: 가로채서 재전송 공격 또는 중간자 공격 등)을 수행해야 함을 의미한다. 그러나 외부 적 또는 악의적인 SN에 의한 사고는 오류를 일으키며, 이에 따라 GHZ 상태는 더 이상 종래와 같이 않다.
- [0084] 다시 말해, 상태는 두 가지를 모두 충족하는 경우에만 GHZ 상태가 된다.
- [0085] 1) 모든 참가자가 Z-기반으로 큐비트를 측정하고 측정 결과가 동일한 경우. 2) 모든 참여자가 X 기반으로 측정을 수행하고 측정 결과의 합이 0 modulo 2인 경우.
- [0086] 따라서 이 두 공격 시나리오는 모두 GHZ 상태의 전송한 3번 및 4번의 검증 설정 중에 감지된다. .
- [0087] 본 개시에 따르면, 프로토콜은 서비스 제공 네트워크(SN)의 도움으로 사용자 단말 간의 양방향 통신을 위한 안전한 통신 채널을 설정하는 방법을 제시한다. 또한 보안 분석은 악의적인 SN 및 외부 적에 대한 이 프로토콜의 견고성을 보여준다.
- [0088] 한편, 효율적인 양자 네트워크를 위해서는 양자 보안 파라미터 추정이 필요하다. 이와 관련하여 종래의 기법은 입자 손실 상황(particle loss regime)에서 추정된 파라미터의 정밀도에서 양자 이점을 제공하지 못한다. 이와 달리, 본 개시에서는 추정된 파라미터의 정밀도를 향상시키기 위해 변형된 보안 추정 프로토콜을 제안한다.
- [0089] 양자 보안 파라미터 추정(quantum secure parameter estimation, QSPE) 프로토콜은 표준 양자 한계(standard quantum limit, SQL)를 초과하는 정밀 스케일링으로 알려지지 않은 물리적 시스템의 연속 파라미터 ϕ 를 추정하고 파라미터의 전송이 무조건 안전하도록 보장하는 것을 목표로 한다. 종래의 프로토콜에서 발신자는 무잡음 채널을 통과하여 원격 시스템에 도달하는 프로브로 알려진 양자 상태를 생성하며 여기서 파라미터 인코딩은 시스템 역학에 의해서만 결정된다. 그러나 실제 적용에서는 발신자와 알 수 없는 시스템 간의 채널에 손실이 발생할 수 있다. 이로 인해 프로브 상태가 잡음이 생기고 결과적으로 추정된 파라미터의 정밀도가 감소한다.
- [0090] 본 개시에서는, 먼저 두 당사자를 위한 HLM 프로토콜을 검토하고 추정의 정확도를 향상시키기 위해 수정된 버전을 제안한다. 구체적으로, 탈분극 채널에서 두 프로토콜의 성능을 분석한다. 수정된 프로토콜은 특히 낮은 입자 체제에서 HLM 프로토콜에 비해 정밀도에서 명확한 이점을 제공한다.
- [0091] 먼저, 양자 계측(quantum metrology)와 탈분극 잡음 채널을 설명한다.
- [0092] [양자 계측]
- [0093] N-partite GHZ 상태는 밀도 행렬 $\rho_0 = |\psi_0\rangle\langle\psi_0|$ 으로 나타낼 수 있으며, 여기서
- $$|\psi_0\rangle = \frac{|0\rangle^{\otimes N} \pm |1\rangle^{\otimes N}}{\sqrt{2}}.$$
- [0094]
- [0095] 상태의 진화는 양자 채널 $\Omega[\rho_0] = \rho_\phi$ 로 나타낼 수 있다. 파라미터 추정은 관찰 가능한 $\hat{X} = [|0\rangle\langle 1|]^{\otimes N} + [|1\rangle\langle 0|]^{\otimes N}$ 을 측정하여 수행된다.
- [0096] 연관된 양자 Cramer-Rao(quantum Cramér-Rao, QCR) 경계는 양자 피셔 정보(FQ) 및 프로브 상태 ν 의 수와 관련하여 다음과 같이 표현될 수 있다.

$$\delta^2 \phi \geq \frac{1}{v F_Q}.$$

[0097]

[0098] 양자 피서 정보는 아래의 식을 사용하여 평가할 수 있습니다.

$$F_Q = \sum_{j,k:\lambda_j+\lambda_k \neq 0} \frac{2|\langle j|\rho'_\phi|k\rangle|^2}{(\lambda_j+\lambda_k)}$$

[0099]

[0100] 여기서 ρ'_ϕ 는 ρ_ϕ 에 대한 ρ_ϕ 의 도함수(derivative)이고 λ_j 및 $|j\rangle$ 는 ρ_ϕ 의 고유값 및 고유벡터이다. 이상적인 경우, 상태는 단일 진화(unitary evolution)를 겪는다.

[0101]

$$\Omega[\rho_0] = U_N \rho_0 U_N^\dagger,$$

[0102]

여기서, $U_N = U^{\otimes N}$ 이다.

[0103]

본 개시에서는 아래를 이용한다.

[0104]

$$U = |0\rangle\langle 0| + e^{i\phi} |1\rangle\langle 1|.$$

[0105]

본 개시에서 제공된 프로토콜의 경우 HLM 프로토콜에 설명된 편향된 단일 인코딩이 아닌 이 단일 인코딩을 사용한다. 이는 분석을 단순화하는 데 도움이 된다.

[0106]

[탈분극 채널]

[0107]

탈분극 채널이 적용된 $d \times d$ 양자 상태 ρ 는 다음과 같이 나타낼 수 있다.

$$\xi[\rho] = (1-p)\rho + p\left(\frac{I}{d}\right).$$

[0108]

[0109]

여기서 $(1-p)$ 는 양자 맵이 이상적인 확률이고 p 는 노이즈 파라미터이다.

[0110]

HLM 프로토콜은 소스 공급자로 제1 사용자 단말, 수신기로 제2 사용자 단말, 및 단말 인코더로 제3 사용자 단말을 포함할 수 있다. 제1 사용자 단말은 프로브 상태를 생성하고 제3 사용자 단말은 알려지지 않은 시스템을 소유하고 파라미터를 인코딩한다. 제2 사용자 단말은 채널의 보안을 확인하고 파라미터 추정 프로세스도 수행한다. 파라미터 추정에 사용되는 상태의 수는 $v\eta P_\psi P_E$ 및 $F_Q = N^2$ 이며, 이를 위의 수식에 적용하면 다음과 같다.

[0111]

$$\delta^2 \phi \geq \frac{2}{v\eta P_\psi P_E N^2}$$

[0112]

여기서 n 는 제2 사용자 장치가 GHZ 기준(basis)으로 인코딩된 상태를 측정할 확률을 나타내고, P_ψ 는 GHZ 상태 생성 확률이며, P_E 는 파라미터 ϕ 로 인코딩할 확률이다. 인수 2는 계산 기반 및 GHZ 기반의 디코이 상태(decoy state)가 수치 상으로 같기 때문이다.

[0113]

[준비 및 배포]

[0114]

제1 사용자 장치는 HLM 프로토콜과 유사한 방식으로 양자 상태를 생성한다. 제1 사용자 장치는 확률 P_ψ 로 프로

브 상태를 생성하고 각각 확률 $(\frac{1-P_\psi}{2})$ 로 $\{|0\rangle^{\otimes N}, |1\rangle^{\otimes N}\}$ 상태를 생성한다. 수정된 프로토콜에서 제1 사용자 장치는 난수 생성기를 사용하여 상태 위치를 수정한다.

[부호화]

제3 사용자 장치는 단일(unitary) U_k 으로 들어오는 상태를 인코딩하고 확률 $1 - P_E$ 로 남긴다.

[추정]

제2 사용자 장치가 상태를 수신한 후, 제1 사용자 장치는 각각의 위치와 신별자를 공개합니다. 제2 사용자 장치는 X 기준으로 GHZ 상태를 측정하고 계산 기준으로 $\{|0\rangle^{\otimes N}, |1\rangle^{\otimes N}\}$ 을 측정한다. 이를 이용하여 제2 사용자 장치는 에러 레이트 를 분석하고 특정 임계치 미만인 경우 위상 파라미터 추정을 계속한다. 파라미터 추정에 사용되는 인코딩된 상태의 수는 $vP_\psi P_E$ 및 $F_Q = N^2$ 이다. 이를 적용한 전술한 연관된 양자 Cramer-Rao(quantum Cramér-Rao, QCR) 경계는 아래와 같다.

$$\delta^2 \phi \geq \frac{1}{vP_\psi P_E N^2}$$

이를 통해 알 수 있듯이 제2 사용자 장치는 보안을 보장하기 위해 무작위 측정을 수행할 필요가 없기 때문에 제1 사용자 장치에 의한 상태의 무작위 순서 지정은 인수 $n/2$ 의 필요성을 제거한다.

전송된 상태가 이상적이지 않으며 탈분극 채널의 영향을 받는 경우, 잡음을 겪게 되며 이에 따른 시스템의 상태는 다음과 같다.

$$\rho_\phi = (1 - p)U_N \rho_0 U_N^\dagger + p(\frac{I}{2^N})$$

이 상태를 전술한 양자 피서 정보에 입력하여 F_Q 및 결과적으로 두 프로토콜의 분산을 평가한다. 도 5는 $p = 0.5$ 인 탈분극 노이즈 하에서 두 프로토콜의 성능을 보여준다. HLM 프로토콜은 $N < 18$ 에 대해 정밀도에서 양자 이점을 제공하지 않는다. 반면에 수정된 HLM 프로토콜은 훨씬 향상된 정밀도 스케일링을 제공하여 SQL을 능가합니다.

따라서, 본 개시는 추정된 파라미터의 정밀도를 향상시키는 보다 효율적인 버전의 HLM 프로토콜을 제안한다. 노이즈의 영향 하에서 이러한 프로토콜의 성능을 분석한 결과, HLM 프로토콜을 수정하면 채널 손실이 있는 경우에도 정밀도에서 양자 이점을 얻을 수 있다. 이에 따라 본 개시의 기법을 이용하면 QSPE 프로토콜의 실질적인 구현을 이룰 수 있다.

양자 암호화는 양자 목록 배포 프로토콜(quantum list distribution protocol)이라는 여러 당사자 간에 상관 목록 값을 안전하게 배포하는 방법을 제공한다. 그러나 잘못된 행동에 대한 프로토콜 복원력에 대한 분석은 아직 부족하다. 특히 큐디트(qudit) 기반 목록 배포 프로토콜은 향후 구현에 가장 실용적이다. 본 개시에서는 당사자의 잘못된 행위에 대한 큐디트 기반 목록 배포 프로토콜 복원력을 분석한다. 잘못된 동작의 두 가지 사례를 소개하고 양자 네트워크 시뮬레이터를 사용하여 시뮬레이션하여 결과를 얻는다. 목록과 목록 배포 시간의 상관관계에 대한 잘못된 동작의 영향을 조사한다. 우리의 결과는 두 경우 모두 목록에서 상관 목록 상관 관계의 정확성을 저하시키는 반면 목록 배포 시간은 두 번째 경우에만 영향을 미친다는 것을 보여준다.

양자 암호화(Quantum cryptography)는 기존의 암호화 방식에 비해 안전하게 정보를 전달하는 새로운 패러다임을 제시한다. 가장 주목할 만한 것 중 하나는 양자 키 분배(Quantum Key Distribution, QKD)로, 무제한 컴퓨팅 리소스를 가진 제3자가 존재하는 경우에도 두 당사자가 비밀 키에 안전하게 동의할 수 있도록 한다. 이는 가로채기 시도(intercept attempt)가 감지되도록 하는 측정 붕괴(measurement collapse)라는 속성 때문이다. 또 다른 중요한 속성은 얽힘(entanglement) 속성으로, 어떤 고전적 상관관계보다 더 강력한 상관관계를 제공한다. 이 두 속성이 결합되어 상관 관계 값을 여러 당사자에게 안전하게 배포할 수 있는 기능을 제공한다.

[0127] 상판 목록의 배포는 다자간 통신 작업에서 많은 어플리케이션을 사용할 수 있도록 해준다. 어플리케이션 중 일부로 비밀 공유, 클록 동기화 및 콘센서스에서 비잔틴 어그리먼트(Byzantine agreement)를 포함한다. 특히, 큐디트 기반 구현은 NISQ(Noisy Intermediate Scale Quantum) 장치에서의 실제 구현에 대한 유망한 결과를 보여준다. 그러나 실제 구현에서 중요한 잘못된 행동에 대한 복원력은 아직 많이 연구되지 않았다. 본 개시에서는 이산 이벤트(Netsquid)를 사용하는 양자 정보를 위한 네트워크 시뮬레이터를 이용하여 큐디트 기반 목록 배포 프로토콜의 결함 동작 시뮬레이션을 수행한다.

[0128] 큐디트 기반 목록 배포 프로토콜은 탐지 가능한 브로드캐스트 문제를 해결하는 데 사용되는 비잔틴 콘센서에 기초한다. 프로토콜은 4자 사례에 대한 것이며 시뮬레이터에서 구현하기 위해 다음과 같이 변형된다.

[0129] 먼저, 당사자 P1은 4자에 대한 큐비트 상태를 준비한다.

$$|\psi\rangle = \frac{1}{2} (|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

[0130]

[0131] 그리고 P1은 기준 c_1 의 값과 목록 값 N_1 을 임의로 결정한다. 여기서 두 값 모두 $\{0, 1, \dots, n-1\}$ 세트 안에 있다. 상대방 P_i 의 경우 c_i 의 값은 c_1 과 같은 집합이지만 N_i 의 값은 $\{0, 1\}$ 집합에 있을 수 있다.

[0132] 모든 당사자 P_i 는 연산자 $U(c_i)$ 를 양자 상태에 적용하며, 이 연산자는,

$$U(c_i) = |0\rangle\langle 0| + \sum_{j=1}^{n-1} e^{i\frac{2\pi}{n}c_i} |j\rangle\langle j|$$

[0133]

[0134] 이고,

[0135] 연산자 $V(N_i)$ 는

$$V(N_i) = \sum_{k=0}^{n-1} e^{i\frac{2\pi}{n}kN_i} |k\rangle\langle k|$$

[0136]

[0137] 이다.

[0138] 모든 P_i 는 다음 당사자인 P_{i+1} 에게 양자 상태를 보낸 다음 모든 $j > i$ 에 대해 c_j 의 결과 발표를 기다린 다음 모든 당사자에게 c_i 값을 알리고 모든 값을 받을 때까지 대기한다.

[0139] 그리고 마지막 당사자 P_n 은 각 큐비트에 아다마르(Hadamard) 게이트를 적용하여 X 기반의 양자 상태를 측정한다. P_n 이 원래 상태를 획득하면 c_n 값을 모든 당사자에게 보내고, 그렇지 않으면 값을 버리고 프로토콜을 다시 시작하라는 메시지를 송신한다.

[0140] c_i 값의 발표는 P_n 에서 P_1 로 역순으로 수행된다. 결과가 $\sum_{i=1}^n c_i \equiv 0 \pmod{n}$ 이면 이번 라운드가 유효한 것으로 간주되고 모든 당사자가 N_i 값을 목록 요소로 기록한다. 그렇지 않으면 값은 폐기되고 다른 라운드가 시작된다. 충분한 길이에 도달하면 프로토콜이 종료된다. 목록 배포 프로토콜 후에 각 당사자는 동일한 길이의 자체 상판 프라이빗 목록을 가진다.

[0141] 잘못된 동작은 목록 기록의 조건과 관련이 있다. 첫 번째 시나리오의 경우 마지막 당사자가 임의의 기본 값을 발표하는 경우를 기본 발표 오류로 표시한다. 두 번째 시나리오의 경우 마지막 당사자는 측정 결과 확인을 건너뛰고 모든 당사자에게 기본 값을 알리는 경우로, 상태 측정 오류로 표시한다. 당사자의 잘못된 행동은 확률적이며 0(무소음)에서 1(항상 결함)까지 다양하다. 본 개시에서는 목록 길이 5000에 대해 시뮬레이션을 실행한다.

[0142] 도 6에 도시된 바와 같이 얻은 결과는 오류 확률이 증가함에 따라 추세가 증가하고 단일 값에 포화됨을 보여준다.

다. 특히, 두 번째 시나리오는 리스트의 상관관계에 더 심각한 영향을 미친다. $N = \left(\sum_i N_i \right) \bmod n$

의 합을 나타내고 C 는 $(\sum_i c_i) \bmod n$ 의 합을 나타낸다. 목록은 $N = 0$ 일 때 올바르게 연관됩니다. 정상적인 조건에서 목록 기록 이벤트는 두 이벤트에 따라 좌우된다.

$$C = 0, \\ |\psi\rangle_{\text{out}} = |\psi\rangle$$

첫 번째 이벤트는 기본 발표 조건이고 두 번째 이벤트는 상태 측정 조건이다. 그리고 목록 정정 상관 확률은 다음과 같다.

$$P(N = 0 | C = 0, |\psi\rangle_{\text{out}} = |\psi\rangle)$$

첫 번째 시나리오에서는 임의의 베이스를 발표함으로써 동작에 사용되는 베이스와 발표된 베이스가 달라진다. 이로 인해 목록의 최대 오류가 0.375가 된다. 두 번째 시나리오에서는 상태 측정 조건을 제거한다. N_i 와 c_i 의 값은 각각 독립적으로 결정되므로 조건부 확률은 $1/4$ 인 $P(N = 0)$ 과 같다. 따라서 상관 오차는 $1 - 1/4 = 0.75$ 이다.

도 6에서 목록 배포 시간에 대한 결과는 평균값에서 약간의 편차를 제외하고 첫 번째 시나리오와 거의 동일하다. 그러나 두 번째 시나리오의 경우 확률이 높아질수록 목록 배포 시간이 줄어든다. 목록 기록 확률은 다음과 같이 표현될 수 있다.

$$P(C = 0, |\psi\rangle_{\text{out}} = |\psi\rangle) = P(|\psi\rangle_{\text{out}} = |\psi\rangle | C = 0)P(C = 0).$$

첫 번째 시나리오는 목록 기록의 조건을 변경하지 않지만, 두 번째 시나리오는 상태 측정 조건을 제거한다. 두 번째 조건을 제거하면 목록 기록 확률이 $P(C = 0)$ 가 되어 목록 기록 확률이 높아지고 평균적으로 목록 배포 시간이 단축된다.

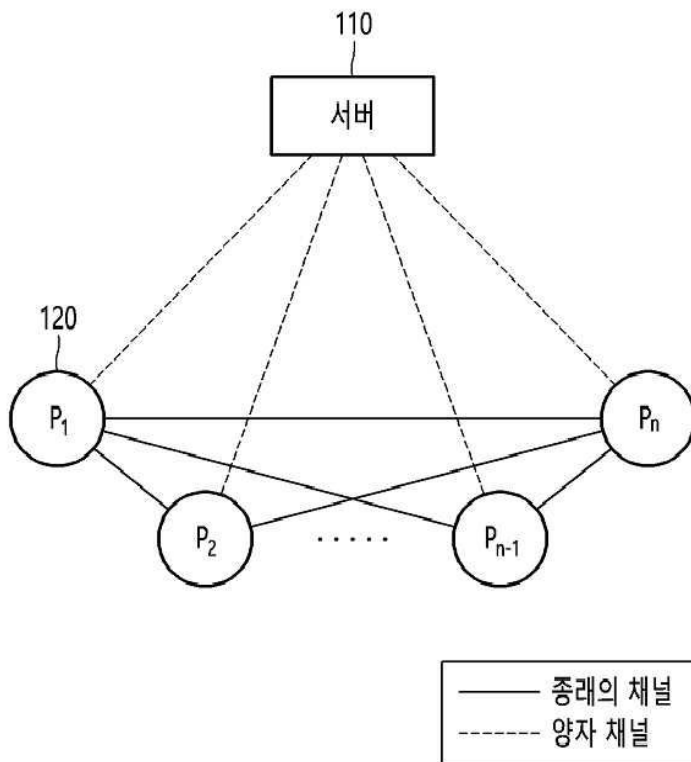
본 개시에서는 큐디트 기반 목록 배포 프로토콜의 결함 동작에 대한 시뮬레이션 및 분석을 제공한다. 여기서 목록 기록 조건과 관련된 두 가지 유형의 오류를 고려한다. 두 경우 모두에 대한 오류 확률에 대한 목록 배포 시간 및 목록 상관 관계의 오류 비율을 플로팅(plot)한다. 목록 상관 오류 결과는 두 오류가 모두 목록 상관에 영향을 미치며 상태 측정 오류가 더 부정적인 영향을 미친다는 것을 나타낸다. 상태 측정 오류는 오류 확률이 증가함에 따라 목록 배포 시간을 감소시킨다.

상기한 실시예들의 설명은 본 개시의 더욱 철저한 이해를 위하여 도면을 참조로 예를 든 것들에 불과하므로, 본 개시의 기술적 사상을 한정하는 의미로 해석되어서는 안될 것이다.

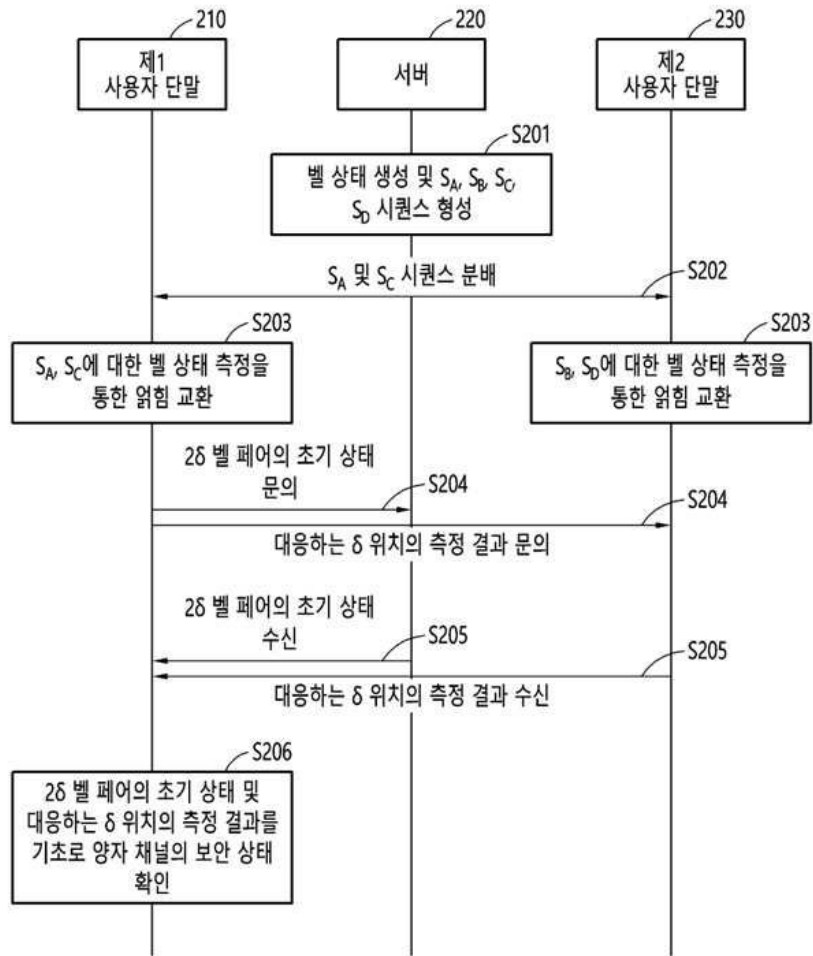
또한, 본 개시가 속하는 기술 분야에서 통상의 지식을 가진 자에게 있어 본 개시의 기본적 원리를 벗어나지 않는 범위 내에서 다양한 변화와 변경이 가능함은 명백하다 할 것이다.

도면

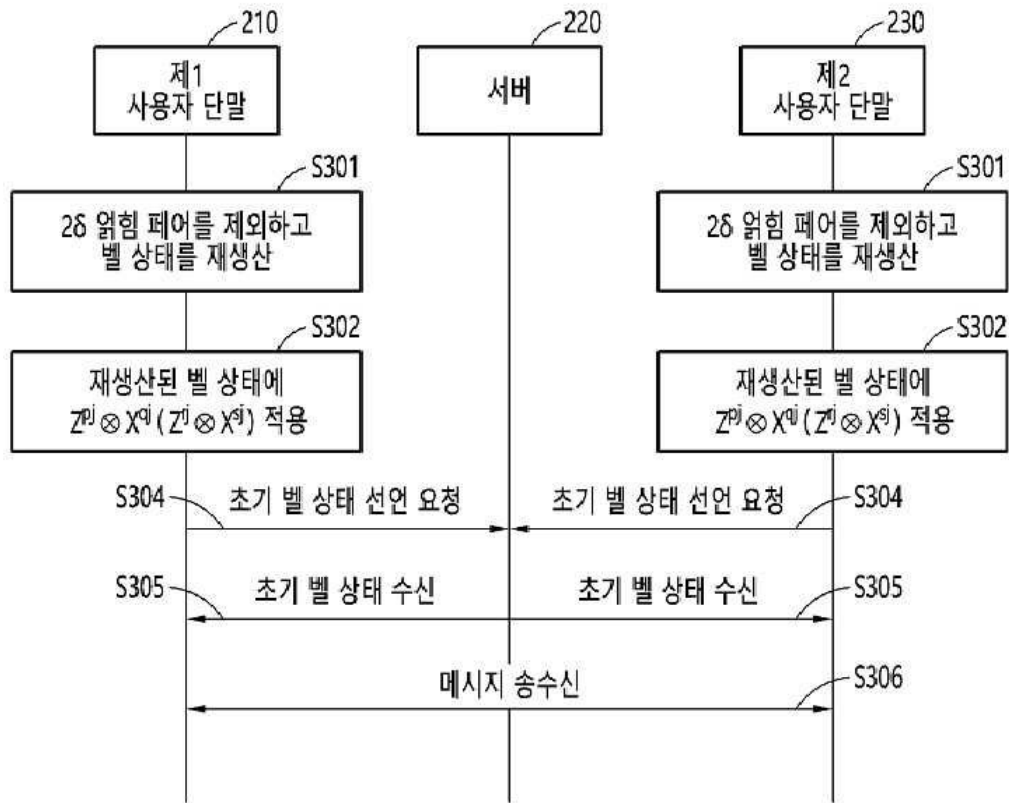
도면1



도면2



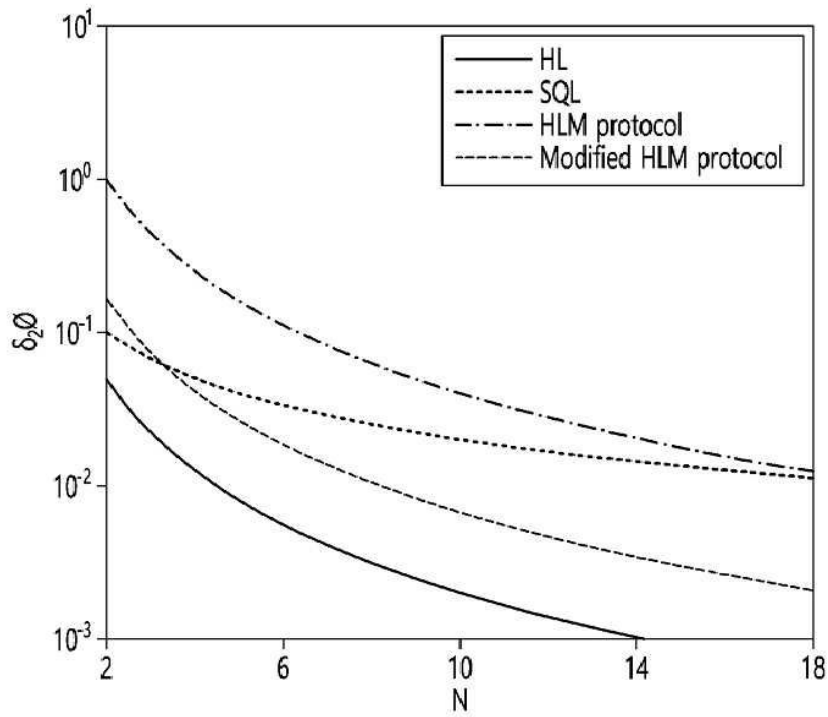
도면3



도면4

	$ \emptyset_{CD}^+\rangle$	$ \emptyset_{CD}^-\rangle$	$ \Psi_{CD}^+\rangle$	$ \Psi_{CD}^-\rangle$
$ \emptyset_{AB}^+\rangle$	A_0	A_1	A_2	A_3
$ \emptyset_{AB}^-\rangle$	A_1	A_0	A_3	A_2
$ \Psi_{AB}^+\rangle$	A_2	A_3	A_0	A_1
$ \Psi_{AB}^-\rangle$	A_3	A_2	A_1	A_0

도면5



도면6

