



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2019-0027217
(43) 공개일자 2019년03월14일

(51) 국제특허분류(Int. Cl.)

H04L 9/08 (2006.01)

(52) CPC특허분류

H04L 9/0858 (2013.01)

(21) 출원번호 10-2017-0113993

(22) 출원일자 2017년09월06일

심사청구일자 2017년09월06일

(71) 출원인

경희대학교 산학협력단

경기도 용인시 기흥구 덕영대로 1732 (서천동, 경희대학교 국제캠퍼스내)

(72) 발명자

신현동

경기도 수원시 영통구 청명로 132, 323동 501호(영통동, 벽산삼익아파트)

정영민

경기도 성남시 분당구 양현로 507, 313동 305호(야탑동, 매화마을주공3단지아파트)

유알리만, 주나이드

경기도 용인시 기흥구 덕영대로 1732, 경희대학교 국제캠퍼스 전자정보관 559호

(74) 대리인

김동용, 김홍석

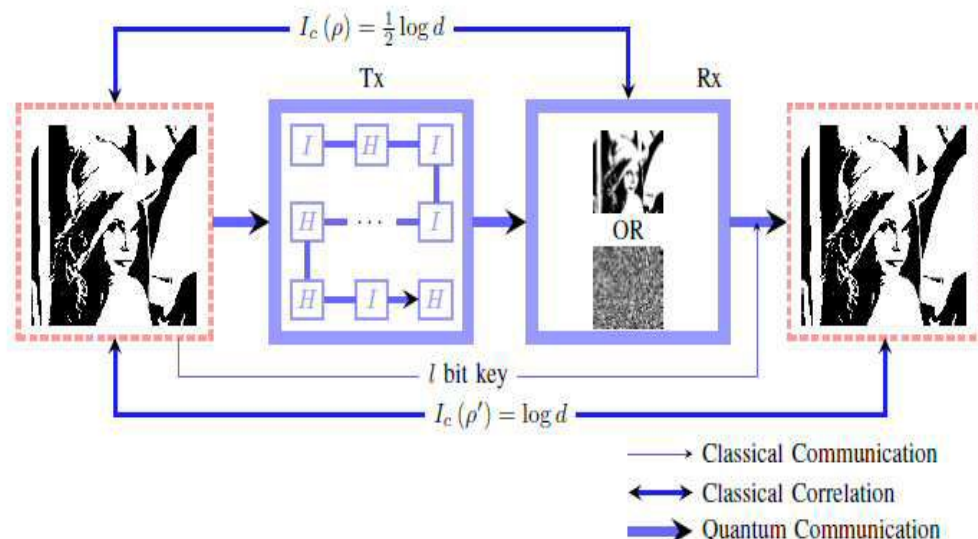
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 양자 정보 보안 방법 및 이를 수행하는 양자 시스템

(57) 요약

본 발명에 따른 양자 정보 보안 방법은, 송신 기기인 제1 기기에 의해 수행되고, 일반 데이터(classical data)를 양자 상태로 인코딩하는 양자 인코딩 단계; 상기 인코딩된 양자 상태에 대해 특정 연산 동작을 적용하는 연산 동작 적용 단계; 및 상기 특정 연산 동작이 적용된 양자 상태의 상기 일반 데이터를 양자 채널(quantum channel)을 통해 제2 기기로 전송하는 정보 전송 단계를 포함하고, 일반 데이터를 양자 상태로 인코딩 및 특정 연산 동작을 통해 양자 채널을 통해 전송함으로써, 양자 정보 보안 방법을 제공할 수 있다.

대표도 - 도3



이 발명을 지원한 국가연구개발사업

과제고유번호 2016R1A2B2014462
 부처명 미래과학창조부
 연구관리전문기관 한국연구재단
 연구사업명 개인연구지원사업(중견연구)
 연구과제명 양자 초업힘을 이용한 하이브리드 양자통신 핵심기술 연구
 기 여 율 1/2
 주관기관 경희대학교 산학협력단
 연구기간 2017.06.01 ~ 2018.05.31

이 발명을 지원한 국가연구개발사업

과제고유번호 R0190-15-2030
 부처명 미래과학창조부
 연구관리전문기관 정보통신기술진흥센터
 연구사업명 정보통신방송연구개발사업
 연구과제명 비밀성증폭 후처리 기술개발
 기 여 율 1/2
 주관기관 경희대학교 산학협력단
 연구기간 2016.07.01 ~ 2017.04.30

명세서

청구범위

청구항 1

양자 정보 보안 방법에 있어서, 상기 방법은 송신 기기인 제1 기기에 의해 수행되고,
일반 데이터(classical data)를 양자 상태로 인코딩하는 양자 인코딩 단계;
상기 인코딩된 양자 상태에 대해 특정 연산 동작을 적용하는 연산 동작 적용 단계; 및
상기 특정 연산 동작이 적용된 양자 상태의 상기 일반 데이터를 양자 채널(quantum channel)을 통해 제2 기기로 전송하는 정보 전송 단계를 포함하는, 양자 정보 보안 방법.

청구항 2

제1 항에 있어서,
언록킹 키(unlocking key)를 일반 채널(classical channel)을 통해 상기 제2 기기로 전송하는 언록킹 키 전송 단계를 더 포함하는, 양자 정보 보안 방법.

청구항 3

제2 항에 있어서,
상기 인코딩된 양자 상태는, n 개의 큐비트의 k 스트링(string)에 대한 큐빙 스트링 $|k\rangle$ 에 대응되고,
상기 특정 연산 동작은 각각의 록킹 부(locking party)가 보유한 비트 키 (t_s)가 $t_s = 0$ 이면 단위 동작(identity operation)이고, $t_s = 1$ 이면 하다마드 동작(Hadamard operation)인 것을 특징으로 하는, 양자 정보 보안 방법.

청구항 4

제3 항에 있어서,
 N 개의 상기 각각의 록킹 부(locking party) s 가 상기 비트 키 (t_s)를 보유한 경우에,
상기 언록킹 키 전송 단계에서, 상기 제2 기기로 전송되는 언록킹 키는 N 개의 비트이고, 상기 정보 전송 단계 및 상기 언록킹 키 전송 단계 이후에 상관의 증폭(Amplification of correlation) r_1 및 연락 상태 정보의 양 r_2 는 $(r_1, r_2) = (2, \log 2^n / 2N)$ 으로 결정되는 것을 특징으로 하는, 양자 정보 보안 방법.

청구항 5

제4 항에 있어서,
상기 각각의 록킹 부는 자신의 비트 키(t_s)를 상호 간에 공유하고,
상기 언록킹 키 전송 단계에서, 상기 제2 기기로 전송되는 언록킹 키는 1 비트인 것을 특징으로 하는, 양자 정보 보안 방법.

청구항 6

양자 정보 보안 방법에 있어서, 상기 방법은 수신 기기인 제2 기기에 의해 수행되고,
언록킹 키(unlocking key)를 일반 채널(classical channel)을 통해 제1 기기로부터 수신하는 언록킹 키 수신 단계; 및
특정 연산 동작이 적용된 양자 상태의 일반 데이터(classical data)를 양자 채널(quantum channel)을 통해 상기 제1 기기로부터 수신하는 정보 수신 단계를 포함하는, 양자 정보 보안 방법.

청구항 7

제6 항에 있어서,

상기 일반 데이터(classical data)는 상기 제1 기기에 의해 양자 상태로 인코딩되고, 상기 인코딩된 양자 상태에 대해 상기 제1 기기에 의해 특정 연산 동작이 적용되어, 제1 상관 정보 ($I_c(p)$)를 가지고,

상기 인코딩된 양자 상태는, n 개의 큐비트의 k 스트링(string)에 대한 큐빙 스트링 $|k\rangle$ 에 대응되고,

상기 특정 연산 동작은 각각의 록킹 부(locking party)가 보유한 비트 키 (ts)가 $ts = 0$ 이면 단위 동작(identity operation)이고, $ts = 1$ 이면 하다마드 동작(Hadamard operation)인 것을 특징으로 하는, 양자 정보 보안 방법.

청구항 8

제7 항에 있어서,

상기 수신된 일반 데이터에 대해 상기 특정 연산 동작과 연관된 연산 동작을 통해 제2 상관 정보 ($I_c(p')$)를 획득하는 단계를 더 포함하는, 양자 정보 보안 방법.

청구항 9

제8 항에 있어서,

상기 언록킹 키 수신 단계에서, 상기 수신되는 언록킹 키는 N 개의 비트이고,

상기 제1 상관 정보 및 상기 제2 상관 정보 ($I_c(p')$)에 따라 결정되는 상관의 증폭(Amplification of correlation) r_1 및 언락 상태 정보의 량 r_2 는 $(r_1, r_2) = (2, \log 2^n/2N)$ 으로 결정되는 것을 특징으로 하는, 양자 정보 보안 방법.

청구항 10

제8 항에 있어서,

상기 획득된 제2 상관 정보 ($I_c(p')$)와 상기 수신된 언록킹 키에 기반하여, 상기 일반 데이터를 포함하는 원시 일반 메시지(original classical message)를 복원하는 데이터 복원 단계를 더 포함하는, 양자 정보 보안 방법.

청구항 11

양자 정보 보안을 수행하는 송신 기기에 있어서,

일반 데이터(classical data)를 양자 상태로 인코딩하고, 상기 인코딩된 양자 상태에 대해 특정 연산 동작을 적용하는 제어부; 및

상기 특정 연산 동작이 적용된 양자 상태의 상기 일반 데이터를 양자 채널(quantum channel)을 통해 수신 기기인 제2 기기로 전송하는 송수신부를 포함하는, 양자 송신 기기.

청구항 12

제11 항에 있어서,

상기 송수신부는 언록킹 키(unlocking key)를 일반 채널(classical channel)을 통해 상기 제2 기기로 전송하는 것을 특징으로 하는, 양자 송신 기기.

청구항 13

제12 항에 있어서,

상기 인코딩된 양자 상태는, n 개의 큐비트의 k 스트링(string)에 대한 큐빙 스트링 $|k\rangle$ 에 대응되고,

상기 특정 연산 동작은 각각의 록킹 부(locking party)가 보유한 비트 키 (ts)가 $ts = 0$ 이면 단위 동작(identity operation)이고, $ts = 1$ 이면 하다마드 동작(Hadamard operation)인 것을 특징으로 하는, 양자 송신

기기.

청구항 14

제13 항에 있어서,

상기 비트 키 (ts)를 저장하도록 구성된 록킹 부(locking party) — 상기 록킹 부는 논리적으로 구분되는 N 개의 록킹 부를 포함하고, 각각의 록킹 부 s는 상기 비트 키 (ts)를 보유함 — 를 더 포함하고,

상기 제2 기기로 전송되는 언록킹 키는 N 개의 비트이고, 상기 일반 데이터 및 상기 전송된 언록킹 키가 전송된 이후, 상관의 증폭(Amplification of correlation) r1 및 연락 상태 정보의 량 r2는 $(r1, r2) = (2, \log 2^n / 2N)$ 으로 결정되는 것을 특징으로 하는, 양자 송신 기기.

청구항 15

제14 항에 있어서,

상기 각각의 록킹 부는 자신의 비트 키(ts)를 상호 간에 공유하고,

상기 제2 기기로 전송되는 언록킹 키는 1 비트인 것을 특징으로 하는, 양자 송신 기기.

청구항 16

양자 정보 보안을 수행하는 수신 기기에 있어서,

언록킹 키(unlocking key)를 일반 채널(classical channel)을 통해 송신 기기인 제1 기기로부터 수신하는 송수신부; 및

특정 연산 동작이 적용된 양자 상태의 일반 데이터(classical data)를 양자 채널(quantum channel)을 통해 상기 제1 기기로부터 수신하도록 상기 송수신부를 제어하는 제어부를 포함하는, 양자 수신 기기.

청구항 17

제16 항에 있어서,

상기 일반 데이터(classical data)는 상기 제1 기기에 의해 양자 상태로 인코딩되고, 상기 인코딩된 양자 상태에 대해 상기 제1 기기에 의해 특정 연산 동작이 적용되어, 제1 상관 정보 ($I_c(p)$)를 가지고,

상기 인코딩된 양자 상태는, n개의 큐비트의 k 스트링(string)에 대한 큐빙 스트링 $|k\rangle$ 에 대응되고,

상기 특정 연산 동작은 각각의 록킹 부(locking party)가 보유한 비트 키 (ts)가 ts = 0이면 단위 동작(identity operation)이고, ts = 1이면 하다마드 동작(Hadamard operation)인 것을 특징으로 하는, 양자 수신 기기.

청구항 18

제17 항에 있어서,

상기 제어부는,

상기 수신된 일반 데이터에 대해 상기 특정 연산 동작과 연관된 연산 동작을 통해 제2 상관 정보 ($I_c(p')$)를 획득하는 것을 특징으로 하는, 양자 수신 기기.

청구항 19

제18 항에 있어서,

상기 송수신부에서 수신되는 상기 언록킹 키는 N 개의 비트이고,

상기 제1 상관 정보 및 상기 제2 상관 정보 ($I_c(p')$)에 따라 결정되는 상관의 증폭(Amplification of correlation) r1 및 연락 상태 정보의 량 r2는 $(r1, r2) = (2, \log 2^n / 2N)$ 으로 결정되는 것을 특징으로 하는, 양자 수신 기기.

청구항 20

제18 항에 있어서,

이미지를 표시하는 디스플레이를 더 포함하고,

상기 제어부는,

상기 획득된 제2 상관 정보 ($I_c(p')$)와 상기 수신된 언로킹 키에 기반하여, 특정 이미지를 포함하는 상기 일반 데이터를 복원하고, 상기 특정 이미지가 상기 디스플레이에 표시되도록 제어하는 것을 특징으로 하는, 양자 수신 기기.

발명의 설명

기술 분야

- [0001] 본 발명은 양자 정보 보안 방법 및 이를 수행하는 양자 시스템에 관한 것이다. 보다 상세하게는, 양자 상태의 양자 시스템에서 다분 일반 데이터(Multipartie classcial data)의 록킹 및 언로킹 방법에 관한 것이다.

배경 기술

- [0002] 양자 통신(quantum communication)의 주된 목적은 일반 정보(classical information) 및 양자 정보(quantum information)의 신뢰성 있는 전송에 있다. 구체적으로, 양자 통신의 한 가지 흥미로운 응용은 양자 시스템을 통한 보안 정보(secret information)의 전달에 있다. 이러한 작업을 위한 가장 널리 사용되는 양자 접근법이 양자 키 분배(QKD: Quantum Key Distribution)이다.
- [0003] 이와 관련하여, 정보 이론 보안을 위하여 QKD를 통해 생성되는 키는 일회용 패드(one-time pad)로 사용된다. 한편, 일회용 패드를 사용하는 암호화를 위한 보안 키의 길이는 암호화될 필요가 있는 메시지의 길이만큼 길어야 한다는 문제점이 있다.
- [0004] 한편, QKD를 통해 생성되는 키가 양자 채널을 통해 전송됨에 따라 전송 가능한 양자 정보의 양이 감소할 수 있다는 문제점이 있다.

발명의 내용

해결하려는 과제

- [0005] 따라서, 본 발명에서 해결하고자 하는 과제는, 양자 정보 보안 방법 및 이를 수행하는 양자 시스템을 제공하는 것을 목표로 한다.
- [0006] 또한, 본 발명에서 해결하고자 하는 과제는, 양자 상태의 양자 시스템에서 다분 일반 데이터(Multipartie classcial data)의 록킹 및 언로킹을 통해 양자 보안을 제공하는 것을 목표로 한다.

과제의 해결 수단

- [0007] 상기와 같은 과제를 해결하기 위한 본 발명에 따른 양자 정보 보안 방법은, 송신 기기인 제1 기기에 의해 수행되고, 일반 데이터(classical data)를 양자 상태로 인코딩하는 양자 인코딩 단계; 상기 인코딩된 양자 상태에 대해 특정 연산 동작을 적용하는 연산 동작 적용 단계; 및 상기 특정 연산 동작이 적용된 양자 상태의 상기 일반 데이터를 양자 채널(quantum channel)을 통해 제2 기기로 전송하는 정보 전송 단계를 포함하고, 일반 데이터를 양자 상태로 인코딩 및 특정 연산 동작을 통해 양자 채널을 통해 전송함으로써, 양자 정보 보안 방법을 제공할 수 있다.
- [0008] 일 실시 예에서, 언로킹 키(unlocking key)를 일반 채널(classical channel)을 통해 상기 제2 기기로 전송하는 언로킹 키 전송 단계를 더 포함할 수 있다.
- [0009] 일 실시 예에서, 상기 인코딩된 양자 상태는, n 개의 큐비트의 k 스트링(string)에 대한 큐빙 스트링 $|k\rangle$ 에 대응되고, 상기 특정 연산 동작은 각각의 록킹 부(locking party)가 보유한 비트 키 (t_s)가 $t_s = 0$ 이면 단위 동작(identity operation)이고, $t_s = 1$ 이면 하다마드 동작(Hadamard operation)인 것을 특징으로 할 수 있다.
- [0010] 일 실시 예에서, N 개의 상기 각각의 록킹 부(locking party) s 가 상기 비트 키 (t_s)를 보유한 경우에, 상기 연

록킹 키 전송 단계에서, 상기 제2 기기로 전송되는 언록킹 키는 N 개의 비트이고, 상기 정보 전송 단계 및 상기 언록킹 키 전송 단계 이후에 상관의 증폭(Amplification of correlation) r_1 및 언락 상태 정보의 량 r_2 는 $(r_1, r_2) = (2, \log 2^n/2N)$ 으로 결정되는 것을 특징으로 할 수 있다.

- [0011] 일 실시 예에서, 상기 각각의 록킹 부는 자신의 비트 키(ts)를 상호 간에 공유하고, 상기 언록킹 키 전송 단계에서, 상기 제2 기기로 전송되는 언록킹 키는 1 비트인 것을 특징으로 할 수 있다.
- [0012] 본 발명의 다른 양상에 따른, 양자 정보 보안 방법은, 수신 기기인 제2 기기에 의해 수행되고, 언록킹 키(unlocking key)를 일반 채널(classical channel)을 통해 제1 기기로부터 수신하는 언록킹 키 수신 단계; 및 특정 연산 동작이 적용된 양자 상태의 일반 데이터(classical data)를 양자 채널(quantum channel)을 통해 상기 제1 기기로부터 수신하는 정보 수신 단계를 포함한다.
- [0013] 일 실시 예에서, 상기 일반 데이터(classical data)는 상기 제1 기기에 의해 양자 상태로 인코딩되고, 상기 인코딩된 양자 상태에 대해 상기 제1 기기에 의해 특정 연산 동작이 적용되어, 제1 상관 정보 ($I_c(p)$)를 가지고, 상기 인코딩된 양자 상태는, n 개의 큐비트의 k 스트링(string)에 대한 큐빙 스트링 $|k\rangle$ 에 대응되고, 상기 특정 연산 동작은 각각의 록킹 부(locking party)가 보유한 비트 키 (ts)가 $ts = 0$ 이면 단위 동작(identity operation)이고, $ts = 1$ 이면 하다마드 동작(Hadamard operation)인 것을 특징으로 할 수 있다.
- [0014] 일 실시 예에서, 상기 수신된 일반 데이터에 대해 상기 특정 연산 동작과 연관된 연산 동작을 통해 제2 상관 정보 ($I_c(p')$)를 획득하는 단계를 더 포함할 수 있다.
- [0015] 일 실시 예에서, 상기 언록킹 키 수신 단계에서, 상기 수신되는 언록킹 키는 N 개의 비트이고, 상기 제1 상관 정보 및 상기 제2 상관 정보 ($I_c(p')$)에 따라 결정되는 상관의 증폭(Amplification of correlation) r_1 및 언락 상태 정보의 량 r_2 는 $(r_1, r_2) = (2, \log 2^n/2N)$ 으로 결정되는 것을 특징으로 할 수 있다.
- [0016] 본 발명의 또 다른 양상에 따른, 양자 정보 보안을 수행하는 송신 기기는, 일반 데이터(classical data)를 양자 상태로 인코딩하고, 상기 인코딩된 양자 상태에 대해 특정 연산 동작을 적용하는 제어부; 및 상기 특정 연산 동작이 적용된 양자 상태의 상기 일반 데이터를 양자 채널(quantum channel)을 통해 수신 기기인 제2 기기로 전송하는 송수신부를 포함한다.
- [0017] 일 실시 예에서, 상기 송수신부는 언록킹 키(unlocking key)를 일반 채널(classical channel)을 통해 상기 제2 기기로 전송하는 것을 특징으로 할 수 있다.
- [0018] 일 실시 예에서, 상기 인코딩된 양자 상태는, n 개의 큐비트의 k 스트링(string)에 대한 큐빙 스트링 $|k\rangle$ 에 대응되고, 상기 특정 연산 동작은 각각의 록킹 부(locking party)가 보유한 비트 키 (ts)가 $ts = 0$ 이면 단위 동작(identity operation)이고, $ts = 1$ 이면 하다마드 동작(Hadamard operation)인 것을 특징으로 할 수 있다.
- [0019] 일 실시 예에서, 상기 비트 키 (ts)를 저장하도록 구성된 록킹 부(locking party) — 상기 록킹 부는 논리적으로 구분되는 N 개의 록킹 부를 포함하고, 각각의 록킹 부 s 는 상기 비트 키 (ts)를 보유함 — 를 더 포함하고, 상기 제2 기기로 전송되는 언록킹 키는 N 개의 비트이고, 상기 일반 데이터 및 상기 전송된 언록킹 키가 전송된 이후, 상관의 증폭(Amplification of correlation) r_1 및 언락 상태 정보의 량 r_2 는 $(r_1, r_2) = (2, \log 2^n/2N)$ 으로 결정되는 것을 특징으로 할 수 있다.
- [0020] 일 실시 예에서, 상기 각각의 록킹 부는 자신의 비트 키(ts)를 상호 간에 공유하고, 상기 제2 기기로 전송되는 언록킹 키는 1 비트인 것을 특징으로 할 수 있다.
- [0021] 본 발명의 또 다른 양상에 따른, 양자 정보 보안을 수행하는 수신 기기는, 언록킹 키(unlocking key)를 일반 채널(classical channel)을 통해 송신 기기인 제1 기기로부터 수신하는 송수신부; 및 특정 연산 동작이 적용된 양자 상태의 일반 데이터(classical data)를 양자 채널(quantum channel)을 통해 상기 제1 기기로부터 수신하도록 상기 송수신부를 제어하는 제어부를 포함한다.
- [0022] 일 실시 예에서, 상기 일반 데이터(classical data)는 상기 제1 기기에 의해 양자 상태로 인코딩되고, 상기 인코딩된 양자 상태에 대해 상기 제1 기기에 의해 특정 연산 동작이 적용되어, 제1 상관 정보 ($I_c(p)$)를 가지고, 상기 인코딩된 양자 상태는, n 개의 큐비트의 k 스트링(string)에 대한 큐빙 스트링 $|k\rangle$ 에 대응되고, 상기 특정 연산 동작은 각각의 록킹 부(locking party)가 보유한 비트 키 (ts)가 $ts = 0$ 이면 단위 동작(identity operation)이고, $ts = 1$ 이면 하다마드 동작(Hadamard operation)인 것을 특징으로 할 수 있다.

- [0023] 일 실시 예에서, 상기 제어부는, 상기 수신된 일반 데이터에 대해 상기 특정 연산 동작과 연관된 연산 동작을 통해 제2 상관 정보 ($I_c(p')$)를 획득하는 것을 특징으로 할 수 있다.
- [0024] 일 실시 예에서, 상기 제어부는, 상기 수신된 일반 데이터에 대해 상기 특정 연산 동작과 연관된 연산 동작을 통해 제2 상관 정보 ($I_c(p')$)를 획득하는 것을 특징으로 할 수 있다.
- [0025] 일 실시 예에서, 상기 송수신부에서 수신되는 상기 언로킹 키는 N 개의 비트이고, 상기 제1 상관 정보 및 상기 제2 상관 정보 ($I_c(p')$)에 따라 결정되는 상관의 증폭(Amplification of correlation) r_1 및 언락 상태 정보의 량 r_2 는 $(r_1, r_2) = (2, \log 2^n / 2N)$ 으로 결정되는 것을 특징으로 할 수 있다.
- [0026] 일 실시 예에서, 이미지를 표시하는 디스플레이를 더 포함하고, 상기 제어부는, 상기 획득된 제2 상관 정보 ($I_c(p')$)와 상기 수신된 언로킹 키에 기반하여, 특정 이미지를 포함하는 상기 일반 데이터를 복원하고, 상기 특정 이미지가 상기 디스플레이에 표시되도록 제어하는 것을 특징으로 할 수 있다.

발명의 효과

- [0027] 본 발명에 따른 방법은, 일반 데이터를 양자 상태로 인코딩 및 특정 연산 동작을 통해 양자 채널을 통해 전송함으로써, 양자 정보 보안 방법을 제공할 수 있다는 장점이 있다.
- [0028] 본 발명에 따른 방법은, 양자 채널로 일반 데이터를 전송하고, 일반 채널로 언로킹 키를 제공하여, 일반 데이터의 록킹 및 언로킹 키를 통해 록킹된 일반 데이터를 복원할 수 있다는 장점이 있다.

도면의 간단한 설명

- [0029] 도 1은 본 발명에 따른 복수의 양자 채널을 포함하는 양자 시스템을 도시한다.
- 도 2는 본 발명에 따른 서버 시스템들의 상세 구성을 도시한다.
- 도 3은 본 발명의 일 실시 예에 따른 양자 정보 보안 방법을 수행하는 양자 송신/수신 기기에서의 통신 채널을 표시하고, 상관 관계를 나타낸 것이다.
- 도 4는 본 발명에 따른 송신 기기인 제1 기기에 의해 수행되는 양자 채널 변환 방법의 흐름도를 나타낸다.
- 도 5는 본 발명에 따른 수신 기기인 제2 기기에 의해 수행되는 양자 채널 변환 방법의 흐름도를 나타낸다.

발명을 실시하기 위한 구체적인 내용

- [0030] 상술한 본 발명의 특징 및 효과는 첨부된 도면과 관련한 다음의 상세한 설명을 통하여 보다 분명해 질 것이며, 그에 따라 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 본 발명의 기술적 사상을 용이하게 실시할 수 있을 것이다. 본 발명은 다양한 변경을 가할 수 있고 여러 가지 형태를 가질 수 있는바, 특정 실시 예들을 도면에 예시하고 본문에 상세하게 설명하고자 한다. 그러나 이는 본 발명을 특정한 개시형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 본 명세서에서 사용한 용어는 단지 특정한 실시 예들을 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다.
- [0031] 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용한다.
- [0032] 제1, 제2등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다.
- [0033] 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. "및/또는" 이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.
- [0034] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미가 있다.
- [0035] 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적

인 의미로 해석되지 않아야 한다.

- [0036] 이하의 설명에서 사용되는 구성요소에 대한 접미사 "모듈", "블록" 및 "부"는 명세서 작성의 용이함만이 고려되어 부여되거나 혼용되는 것으로서, 그 자체로 서로 구별되는 의미 또는 역할을 갖는 것은 아니다.
- [0037] 이하, 본 발명의 바람직한 실시 예를 첨부한 도면을 참조하여 당해 분야에 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 설명한다. 하기에서 본 발명의 실시 예를 설명함에 있어, 관련된 공지의 기능 또는 공지의 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략한다.
- [0038] 이하, 본 발명에 따른 양자 채널 변환 방법 및 양자 채널 변환 시스템에 대해 살펴보기로 하자.
- [0039] 이와 관련하여, 도 1은 본 발명에 따른 복수의 양자 채널을 포함하는 양자 시스템을 도시한다. 도 1에 도시된 바와 같이, 양자 시스템은 복수의 서버 시스템을 포함하고, 편의상 제1 서버 시스템(100)과 제2 서버 시스템(200)이 포함된 것으로 표현할 수 있다. 하지만, 상기 제1 및 제2 서버 시스템(100, 200)에만 한정되는 것이 아니라, 임의의 개수의 서버 시스템 간에도 적용될 수 있다. 한편, 상기 제1 및 제2 서버 시스템(100, 200)은 임의의 양자 기기일 수 있고, 하나의 양자 기기 내의 서로 다른 컴포넌트일 수 있다. 예를 들어, 제1 서버 시스템(100)은 사용자 Alice 측에 해당하는 기기이고, 송신 기기로 제1 기기(100)로 지칭될 수 있다. 유사하게, 제2 서버 시스템(200)은 사용자 Bob 측에 해당하는 기기이고, 수신 기기로 제2 기기(200)로 지칭될 수 있다. 한편, 편의상 제1 기기(100)가 송신 기기로, 제2 기기(200)가 수신 기기로 표시되었지만, 그 역도 성립할 수 있다. 또한, 경우에 따라, 제1 기기(100)가 송신 또는 수신 기기로 동작함에 따라, 제2 기기(200)는 이에 대응하여 수신 또는 송신 기기로 동작할 수 있다.
- [0040] 한편, 도 2는 본 발명에 따른 서버 시스템들의 상세 구성을 도시한다. 도 2에 도시된 바와 같이, 제1 서버 시스템(100)은 제어부(110), 송수신부(120), 및 메모리(130)를 포함한다. 또한, 제2 서버 시스템(200)은 제어부(210), 송수신부(220), 메모리(230), 및 디스플레이(240)를 포함한다. 여기서, 송수신부(120, 220)는 양자 채널(quantum channel)을 이용하는 양자 송수신부(121, 221)일 수 있다. 또한, 송수신부(120, 220)는 일반 채널(classical channel)을 이용하는 일반 송수신부(122, 222)를 포함할 수 있다. 한편, 메모리(130, 230)는 양자 정보를 저장하는 양자 메모리일 수 있다. 또한, 메모리(130, 230)는 일반 정보를 저장하는 일반 메모리를 포함할 수 있다. 여기서, 메모리(130, 230)가 데이터의 록킹/언록킹과 관련된 비트 키를 저장하는 경우에 특히, 록킹 부(locking party, locking unit)으로 지칭될 수 있다.
- [0041] 한편, 도 3은 본 발명의 일 실시 예에 따른 양자 정보 보안 방법을 수행하는 양자 송신/수신 기기에서의 통신 채널을 표시하고, 상관 관계를 나타낸 것이다.
- [0042] 도 2 및 도 3을 참조하여, 본 발명에 따른 양자 정보 보안 방법과 이를 수행하는 양자 송신/수신 기기를 살펴보면 다음과 같다.
- [0043] 먼저, 송신 기기에 해당하는 제1 기기(100)에서의 동작에 대해 살펴보면 다음과 같다.
- [0044] 제어부(110)는 일반 데이터(classical data)를 양자 상태로 인코딩하고, 상기 인코딩된 양자 상태에 대해 특정 연산 동작을 적용한다.
- [0045] 송수신부(120), 특히 양자 송수신부(121)는 상기 특정 연산 동작이 적용된 양자 상태의 상기 일반 데이터를 양자 채널(quantum channel)을 통해 수신 기기인 제2 기기(200)로 전송한다. 또한, 송수신부(120), 특히 일반 송수신부(122)는 언록킹 키(unlocking key)를 일반 채널(classical channel)을 통해 상기 제2 기기(200)로 전송하는 것을 특징으로 할 수 있다.
- [0046] 이때, 상기 인코딩된 양자 상태는, n 개의 큐비트의 k 스트링(string)에 대한 큐빙 스트링 $|k\rangle$ 에 대응될 수 있다. 한편, 상기 특정 연산 동작은 각각의 록킹 부(locking party)가 보유한 비트 키 (t_s)가 $t_s = 0$ 이면 단위 동작(identity operation)이고, $t_s = 1$ 이면 하다마드 동작(Hadamard operation)인 것을 특징으로 할 수 있다.
- [0047] 메모리(130), 특히 록킹 부(locking party)는 상기 비트 키 (t_s)를 저장하도록 구성된다. 이때, 상기 록킹 부는 논리적으로 구분되는 N 개의 록킹 부를 포함하고, 각각의 록킹 부 s 는 상기 비트 키 (t_s)를 보유할 수 있다.
- [0048] 한편, 상기 제2 기기(200)로 전송되는 언록킹 키는 N 개의 비트이고, 상기 일반 데이터 및 상기 전송된 언록킹 키가 전송된 이후, 상관의 증폭(Amplification of correlation) r_1 및 언락 상태 정보의 량 r_2 는 $(r_1, r_2) = (2, \log 2^n / 2N)$ 으로 결정될 수 있다. 이에 따라, 언록킹 키의 개수가 증가함에 따라 언락 상태 정보의 량이 감

소하므로, 원시 데이터(일반 데이터)의 복원이 가능하게 된다.

- [0049] 또한, 메모리(130), 특히 록킹 부(locking party)는 자신의 비트 키(ts)를 상호 간에 공유하고, 상기 제2 기기(200)로 전송되는 언록킹 키는 1 비트일 수 있다. 이에 따라, 상기 제2 기기(200)로 전송되는 원시 데이터(일반 데이터)의 량의 증가에도 불구하고, 암호화를 위한 보안 키의 길이는 일정한 값을 가질 수 있다. 즉, 암호화를 위한 보안 키의 길이는 암호화될 필요가 있는 메시지의 길이만큼 길어야 한다는 문제점이 해결될 수 있고, 이에 따라 일회용 패드를 사용하는 암호화방식에 있어서도 언록킹을 위한 보안 키의 길이가 증가함을 방지할 수 있다.
- [0050] 다음으로, 수신 기기인 제2 기기(200)의 측면에서, 양자 정보 보안에 대해 살펴보면 다음과 같다.
- [0051] 송수신부(220), 특히 일반 송수신부(222)는 언록킹 키(unlocking key)를 일반 채널(classical channel)을 통해 송신 기기인 제1 기기(100)로부터 수신할 수 있다.
- [0052] 한편, 제어부(210)는 특정 연산 동작이 적용된 양자 상태의 일반 데이터(classical data)를 양자 채널(quantum channel)을 통해 상기 제1 기기(100)로부터 수신하도록 송수신부(220), 특히 양자 송수신부(221)를 제어한다.
- [0053] 이때, 상기 일반 데이터(classical data)는 상기 제1 기기(100)에 의해 양자 상태로 인코딩되고, 상기 인코딩된 양자 상태에 대해 상기 제1 기기(100)에 의해 특정 연산 동작이 적용되어, 제1 상관 정보($I_c(p)$)를 가질 수 있다. 한편, 상기 인코딩된 양자 상태는, n 개의 큐비트의 k 스트링(string)에 대한 큐빙 스트링 $|k\rangle$ 에 대응되고, 상기 특정 연산 동작은 각각의 록킹 부(locking party)가 보유한 비트 키 (ts)가 $ts = 0$ 이면 단위 동작(identity operation)이고, $ts = 1$ 이면 하다마드 동작(Hadamard operation)인 것을 특징으로 할 수 있다.
- [0054] 또한, 제어부(210)는 상기 수신된 일반 데이터에 대해 상기 특정 연산 동작과 연관된 연산 동작을 통해 제2 상관 정보 ($I_c(p')$)를 획득할 수 있다. 여기서, 상기 연관된 연산 동작은 상기 특정 연산 동작의 역변환(inverse transform)일 수 있다. 또는, 상기 연관된 연산 동작은 상기 특정 연산 동작과 동일 (또는 유사)한 연산 동작일 수 있다.
- [0055] 한편, 송수신부(220), 특히 일반 송수신부(222)에서 수신되는 상기 언록킹 키는 N 개의 비트일 수 있다. 이와 관련하여, 상기 제1 상관 정보 및 상기 제2 상관 정보 ($I_c(p')$)에 따라 결정되는 상관의 증폭(Amplification of correlation) r_1 및 언락 상태 정보의 량 r_2 는 $(r_1, r_2) = (2, \log 2^n/2N)$ 으로 결정되는 것을 특징으로 할 수 있다.
- [0056] 메모리(230), 특히 록킹 부(locking party)는 제1 기기(100)의 메모리(130)로부터 전달된 상기 비트 키 (ts)를 저장하도록 구성될 수 있다. 또한, 메모리(230)는 제1 기기(100)로부터 전송된 양자 정보 (또는 이와 관련된 정보)를 저장하도록 구성될 수 있다.
- [0057] 디스플레이(240)는 이미지를 표시하도록 구성된다. 이와 관련하여, 제어부(210)는, 상기 획득된 제2 상관 정보 ($I_c(p')$)와 상기 수신된 언록킹 키에 기반하여, 특정 이미지를 포함하는 상기 일반 데이터를 복원하고, 상기 특정 이미지가 상기 디스플레이(240)에 표시되도록 제어할 수 있다.
- [0058] 전술된, 양자 송신 기기 (제1 기기(100)) 및 양자 수신 기기 (제2 기기(200))에서의 양자 보안 변환 방법에 대해서 상세히 설명하면 아래와 같다. 구체적으로, 양자 상태의 일반 상관의 록킹 절차 및 이와 관련된 용어(terminology)에 대해 살펴보기로 한다.
- [0059] 이와 관련하여, 양호한 상관 측정에 의해 만족되어야 하는 공리 특성들(axiomatic properties)이 있다. 이러한 중요한 특성은 증가 비례(*incremental proportionality*)의 원칙이라 지칭될 수 있다. 이러한 특성은 양 주체들(two parties) 간의 1개의 큐비트 또는 21개의 비트의 전송이 21개의 비트 이상에 의해 기존 상관(preexisting correlation)을 증가시키지 않아야 한다는 것이다. 하지만, 양자 상태에서 일반 데이터 록킹은 이러한 특성을 상당히 위반한다. 본 발명에서 고려하는 상관은 제1 기기(Alice의 기기)(100)와 제2 기기(Bob의 기기)(200) 측에 대한 로컬 측정을 통해 최대화되는 양자 상태 ρ_{AB} 의 일반 상호 정보(classical mutual information)이고, 아래의 수학적 식 1과 같이 주어진다.

수학식 1

$$I_c(\rho) = \max_{M_A \otimes M_B} I(A; B)$$

[0060]

[0061]

여기서, $I(A; B) = H(A) + H(B) - H(AB)$ 은 일반 상호 정보를 나타내고, 여기서 $H(\cdot)$ 는 샤논 엔트로피이다. 이러한 상관의 표시(notion)를 이용하여, 본원에서는 두 개의 양자 기기인 제1 기기(Alice의 기기)(100)와 제2 기기(Bob의 기기)(200)를 고려한다. 제1 기기(100)는 n 개의 큐비트의 스트링 k 를 생성한다. 이러한 큐비트의 스트링은 정규 직교 기저(orthonormal basis)로 준비(prepare)된다는 점에서 일반 데이터라고 할 수 있고, 각 큐비트는 두 개의 기저 벡터 상태 중 하나일 수 있다. 이제, 제1 기기(100)는 제2 기기(200)로 비트 $t=0, 1$ 의 상태로 $|k\rangle$ 또는 $H^{\otimes n}|k\rangle$ 을 전송할 수 있고, 여기서 H 는 아래의 수학식 2와 같이 주어지는 하다마드(Hadamard) 변환을 나타낸다.

수학식 2

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

[0062]

[0063]

여기서, $\otimes$ 는 텐서(Kronecker) 곱을 나타낸다. 제2 기기(200)의 관점에서는, 제2 기기(200)는 밀도 연산자 ρ 에 의해 표시되는 상태들 $\{|k\rangle, H^{\otimes n}|k\rangle\}$ 의 균일 앙상블을 보유한다. 이러한 경우에, 초기 상관 $I_c(\rho) = 1/2 * \log d$ 로 주어지고, 여기서 $d = 2^n$ 이다. 일단, 제1 기기(100)가 일반 비트를 제2 기기(200)로 전송하면, 제2 기기(200)는 ρ 에 대해 대응하는 연산 (I 또는 H)를 적용하여 ρ' 을 획득할 수 있다. 이러한 연산 이후에, 제1 기기(100)와 제2 기기(200) 간의 상관은 $1/2 * \log d$ 로 감소된다.

[0064]

이러한 증가 비례의 위반 정도를 정량화하기 위한 두 가지 감도 지수(figure of merit)가 아래와 같이 제시될 수 있다.

[0065]

- 상관의 증폭(Amplification of correlation)

$$r_1 = I_c(\rho') / I_c(\rho)$$

[0066]

[0067]

- 키 사이즈에 상대적인 언락 상태 정보의 량(amount of unlocked information)

$$r_2 = \frac{I_c(\rho') - I_c(\rho)}{l}$$

[0068]

[0069]

전술된 예시에 대하여, $(r_1, r_2) = (2, \log 2^n / 2N)$ 으로 주어질 수 있다. 이는 언락 키의 전송이 송신 기기인 제1 기기(100)와 수신 기기인 제2 기기(200) 간의 상관을 2배(r_1) 만큼 증가시킴을 보여준다. 또한, 언락 키에 상대적인 언락 상태 정보의 량은 값 $d = 2^n$ (n 은 큐비트의 수)의 값을 증가시켜 임의로 크게 할 수 있다.

[0070]

다음으로, 본 발명의 또 다른 실시 예에 따른 양자 정보 보안 방법에 대해 살펴보기로 하자. 즉, 양자 상태에서 일반 상관을 록킹하는 방식이 제안되고, 여기서 $N+1$ 개의 엔티티(또는 parties)가 록킹 동작에 관여한다. 록킹 이후에, 록킹된 스트링이 수신 기기인 제2 기기(200)로 전송된다. 제2 기기(200)가 록킹된 스트링을 수신하였을 때인 이 시점에서의 상관이 초기 상관(initial correlation)이라고 불리운다. 최종 상관($I_c(\rho')$)를 언락하기 위해 길이 l 의 언락 키가 제2 기기(200)로 전송될 필요가 있다.

[0071]

이러한 가정에 근거하여, 전술된 감도 지수에 대하여 본 실시 예의 성능을 평가하면 다음과 같다.

[0072] 제안된 방식에서, 송신 측인 제1 기기(100)의 각 록킹 부(locking party) s가 자신의 비트 키 ts를 보유하고 있고, 비트 키 ts는 하다마드 변환이 적용된 상태에 있다고 하자. 이때, 비트 키 ts는 전술된 바와 같이, 복수의 비트일 수 있고, 또한, 엔티티(parties) 간에 정보를 공유할 수 있고, 하나의 비트로 구성될 수도 있다. 한편, 큐빗 스트링 $|k\rangle$ 에 대한 전체 록킹 동작은 아래의 수학적 식 3과 같이 표현될 수 있다.

수학적 식 3

$$(H^{\otimes n})^{t_1} (H^{\otimes n})^{t_2} \dots (H^{\otimes n})^{t_N} |k\rangle$$

[0073]

[0074] 이때, 이러한 록킹 동작 이후에 생성된 스트링은 동일한 확률을 갖는 $|k\rangle$ 또는 $H^{\otimes n}|k\rangle$ 중 하나일 수 있다. 따라서, 제1 기기(100)와 제2 기기(200) 간의 초기 상관관계는 이전 실시 예에서의 원래 방식과 동일할 수 있다. 한편, 큐빗 스트링에서 숨겨진 상관관계(hidden correlation)를 언락하기 위해, N 비트의 언락 키가 제2 기기(200)로 전송될 필요가 있다. 그러므로, $(r_1, r_2) = (2, \log 2^{n/2N})$ 의 관계가 성립된다.

[0075] 한편, 록킹 부들이 상호 간에 신뢰하고 그들의 록킹 비트들 ts를 상호 간에 알고 있다면, 단지 하나의 비트를 이용하여 결합된 록킹 동작(combined locking action)이 제2 기기(200)로 전송될 수 있다. 증가 비례 특성의 관점에서, 초기 상관관계에서 최종 상관관계 간의 차이는 일반 키 사이즈 I보다 크지 않아야 한다.

[0076] 제안된 실시 예에서, $I = N$ 비트의 언락 키의 전송은 $1/2 \cdot \log d$ 에서 $\log d$ 로 상관 값을 2배 증가시킨다. 따라서, $N < n/2$ 를 만족하지만 하면 (즉, 언락 키의 비트 개수가 큐빗 개수의 절반보다 작으면), 증가 비례 특성은 위반된다.

[0077] 이와 관련하여, 도 3은 전술된 바와 같이, 본 발명의 일 실시 예에 따른 양자 정보 보안 방법을 수행하는 양자 송신/수신 기기에서의 통신 채널을 표시하고, 상관 관계를 나타낸 것이다. 즉, 도 3은 제안된 방식을 나타내고, 구체적으로, 예시적인 록킹된 일반 데이터로서 바이너리 이미지 '레나(lena)'를 이용하는 시뮬레이션 결과를 나타낸다. 바이너리 이미지는 제1 기기(100)에서 양자 상태 $|k\rangle$ 로 인코딩되고, 이후에 록킹 부에 의해 동작된다. 각 록킹 부는 보유한 상태에 대해 (예컨대, $t_s = 0$ 에 대하여) 단위 동작(identity operation), 또는 (예컨대, $t_s = 1$ 에 대하여) 하다마드 동작(Hadamard operation)을 적용한다. 록킹된 이미지는 수신기인 제2 기기(200)로 전송되고, 원래 일반 메시지와 일반 상관관계는 실제 데이터 양의 단지 절반에 불과하다. 일단 언락된 키 I이 일반 채널을 통해 수신 기기(Rx)인 제2 기기(200)로 전송되면, 완전 상관관계(full correlation)가 언락되고 원래 일반 메시지가 복원된다.

[0078] 이상에서는, 양자 상태에서 일반 데이터의 록킹에 복수의 주체들이 관여하는 시나리오의 확장된 방식에 대해 논의되었다. 이와 관련된 제안된 방식의 해석 및 구조는 관여된 주체의 수가 큰 경우에도 증가된 비례 특성이 여전히 위반된다는 것을 보여준다. 그러나, 이러한 위반과 관련된 특성을 보장하기 위해, 전술된 바와 같이 록킹된 상관관계 n의 크기, 및 관여된 주체들의 수 N 사이의 특정 관계가 만족되어야 한다. 이러한 증가 비례 특성의 위반으로 인해, 양자 영역의 이러한 방식의 독점성과 양자 물리에서의 현상을 모방하는 것의 불가능성을 확인해준다. 향후에는, 각 록킹 부의 바이너리 선택 (I 또는 H)이 고정 회전 동작(fixed rotation operation)에 의해 대체될 수 있을 것으로 기대된다. 이와 관련하여, 고정 회전 동작은 록킹 파라미터일 수 있다.

[0079] 한편, 전술된 내용을 토대로, 본 발명의 다른 측면에 따른 양자 보안 방법에 대해 살펴보면 다음과 같다. 이와 관련하여, 도 4는 본 발명에 따른 송신 기기인 제1 기기에 의해 수행되는 양자 채널 변환 방법의 흐름도를 나타낸다. 한편, 도 5는 본 발명에 따른 수신 기기인 제2 기기에 의해 수행되는 양자 채널 변환 방법의 흐름도를 나타낸다. 한편, 전술된 내용은 이하에서 설명되는 양자 보안 방법과 결합하여 이용될 수 있다.

[0080] 도 5를 참조하면, 송신 기기에서의 양자 보안 방법은 양자 인코딩 단계(S110), 연산 동작 적용 단계(S120), 언락 키 전송 단계(S130) 및 정보 전송 단계(S140)를 포함한다. 여기서, 전술된 단계들은 나열된 단계에 한정되는 것이 아니라, 응용에 따라 자유롭게 변형 가능하다. 예를 들어, 언락 키 전송 단계(S130)는 제2 기기가 수신된 정보를 언락키하기 이전에만 이루어지면 될 뿐, 반드시 연산 동작 적용 단계(S120) 이후에 이루어져야 하는 것은 아니다.

[0081] 양자 인코딩 단계(S110)에서, 일반 데이터(classical data)가 양자 상태로 인코딩된다. 이때, 상기 인코딩된 양

자 상태는, n 개의 큐비트의 k 스트링(string)에 대한 큐빙 스트링 $|k\rangle$ 에 대응될 수 있다.

- [0082] 한편, 연산 동작 적용 단계(S120)에서, 상기 인코딩된 양자 상태에 대해 특정 연산 동작이 적용된다. 한편, 상기 특정 연산 동작은 각각의 록킹 부(locking party)가 보유한 비트 키(ts)가 $ts = 0$ 이면 단위 동작(identity operation)이고, $ts = 1$ 이면 하다마드 동작(Hadamard operation)인 것을 특징으로 할 수 있다.
- [0083] 또한, 언록킹 키 전송 단계(S130)에서, 언록킹 키(unlocking key)를 일반 채널(classical channel)을 통해 상기 제2 기기로 전송한다.
- [0084] 한편, 정보 전송 단계(S140)에서, 상기 특정 연산 동작이 적용된 양자 상태의 상기 일반 데이터를 양자 채널(quantum channel)을 통해 제2 기기로 전송된다. 이때, N 개의 상기 각각의 록킹 부(locking party) s 가 상기 비트 키 (ts)를 보유한 경우에는 다음과 같이 상관 상태가 변경될 수 있다. 즉, 상기 언록킹 키 전송 단계(S130)에서, 상기 제2 기기로 전송되는 언록킹 키는 N 개의 비트이고, 상기 언록킹 키 전송 단계(S130) 및 상기 정보 전송 단계(S140) 이후에 상관의 증폭(Amplification of correlation) $r1$ 및 연락 상태 정보의 량 $r2$ 는 $(r1, r2) = (2, \log 2^n / 2N)$ 으로 결정되는 것을 특징으로 할 수 있다.
- [0085] 또한, 본 발명의 다른 실시 예에 따르면, 상기 각각의 록킹 부는 자신의 비트 키(ts)를 상호 간에 공유하고, 상기 언록킹 키 전송 단계(S130)에서, 상기 제2 기기로 전송되는 언록킹 키는 1 비트인 것을 특징으로 할 수 있다.
- [0086] 도 6을 참조하면, 수신 기기에서의 양자 보안 방법은 언록킹 키 수신 단계(S210), 정보 수신 단계(S220), 제2 상관 정보 획득 단계(S230) 및 데이터 복원 단계(S240)를 포함한다. 여기서, 전송된 단계들은 나열된 단계에 한정되는 것이 아니라, 응용에 따라 자유롭게 변형 가능하다. 예를 들어, 언록킹 키 수신 단계(S210)가 반드시 가장 먼저 수행되어야 하는 것은 아니고, 데이터 복원 단계(S240) 이전에만 언록킹 키가 수신되면 된다.
- [0087] 언록킹 키 수신 단계(S210)에서, 언록킹 키(unlocking key)를 일반 채널(classical channel)을 통해 제1 기기로부터 수신한다. 상기 언록킹 키 수신 단계(S210)에서 상기 수신되는 언록킹 키는 N 개의 비트일 수 있다. 또는, 전송된 바와 같이, 록킹 부(locking party)가 자신의 비트 키(ts)를 상호 간에 공유하면, 언록킹 키는 1 비트일 수 있다. 이에 따라, 상기 제2 기기로 전송되는 원시 데이터(일반 데이터)의 량의 증가에도 불구하고, 암호화를 위한 보안 키의 길이는 일정한 값을 가질 수 있다.
- [0088] 정보 수신 단계(S220)에서, 특정 연산 동작이 적용된 양자 상태의 일반 데이터(classical data)를 양자 채널(quantum channel)을 통해 상기 제1 기기로부터 수신한다. 이때, 상기 일반 데이터(classical data)는 상기 제1 기기에 의해 양자 상태로 인코딩되고, 상기 인코딩된 양자 상태에 대해 상기 제1 기기에 의해 특정 연산 동작이 적용될 수 있다. 이에 따라, 상기 일반 데이터는 제1 상관 정보 ($Ic(p)$)를 가질 수 있고, 필요에 따라 상기 제1 상관 정보 ($Ic(p)$)는 제2 기기로 전달될 수 있다. 한편, 상기 인코딩된 양자 상태는, n 개의 큐비트의 k 스트링(string)에 대한 큐빙 스트링 $|k\rangle$ 에 대응되고, 상기 특정 연산 동작은 각각의 록킹 부(locking party)가 보유한 비트 키 (ts)가 $ts = 0$ 이면 단위 동작(identity operation)이고, $ts = 1$ 이면 하다마드 동작(Hadamard operation)인 것을 특징으로 할 수 있다.
- [0089] 제2 상관 정보 획득 단계(S230)에서, 상기 수신된 일반 데이터에 대해 상기 특정 연산 동작과 연관된 연산 동작을 통해 제2 상관 정보 ($Ic(p')$)를 획득할 수 있다. 이와 관련하여, 상기 제1 상관 정보 및 상기 제2 상관 정보 ($Ic(p')$)에 따라 결정되는 상관의 증폭(Amplification of correlation) $r1$ 및 연락 상태 정보의 량 $r2$ 는 $(r1, r2) = (2, \log 2^n / 2N)$ 으로 결정될 수 있다.
- [0090] 데이터 복원 단계(S240)에서, 상기 획득된 제2 상관 정보 ($Ic(p')$)와 상기 수신된 언록킹 키에 기반하여, 상기 일반 데이터를 포함하는 원시 일반 메시지(original classical message)를 복원할 수 있다.
- [0091] 한편, 본 발명의 양자 정보 보안 방법 및 이를 수행하는 양자 기기들은 전송 장치와 수신 장치 간의 보안 통신에 활용될 수 있다. 이때, 복수 개의 비트, 또는 경우에 따라 단 한 비트를 갖는 보안 키가 요구되고, 보안 키를 이용하여 록킹된 메시지를 연락할 수 있다.
- [0092] 이러한 본 발명에 따른 기대 효과는, 양자 통신 네트워크에서 대상들 간의 효율적인 보안 통신이 가능하다는 점이다. 한편, 본 발명의 기술 사업화 전망은 양자 통신을 수행하는 양자 네트워크에서 보안 통신 시스템을 제공할 수 있다는 것이다.
- [0093] 전송된 본 발명의 적어도 일 실시 예에 따르면, 일반 데이터를 양자 상태로 인코딩 및 특정 연산 동작을 통해

양자 채널을 통해 전송함으로써, 양자 정보 보안 방법을 제공할 수 있다는 장점이 있다.

[0094] 또한, 본 발명의 적어도 일 실시 예에 따르면, 양자 채널로 일반 데이터를 전송하고, 일반 채널로 언로킹 키를 제공하여, 일반 데이터의 록킹 및 언로킹 키를 통해 록킹된 일반 데이터를 복원할 수 있다는 장점이 있다.

[0095] 소프트웨어적인 구현에 의하면, 본 명세서에서 설명되는 절차 및 기능뿐만 아니라 각각의 구성 요소들은 별도의 소프트웨어 모듈로도 구현될 수 있다. 상기 소프트웨어 모듈들 각각은 본 명세서에서 설명되는 하나 이상의 기능 및 작동을 수행할 수 있다. 적절한 프로그램 언어로 쓰여진 소프트웨어 어플리케이션으로 소프트웨어 코드가 구현될 수 있다. 상기 소프트웨어 코드는 메모리에 저장되고, 제어부(controller) 또는 프로세서(processor)에 의해 실행될 수 있다.

부호의 설명

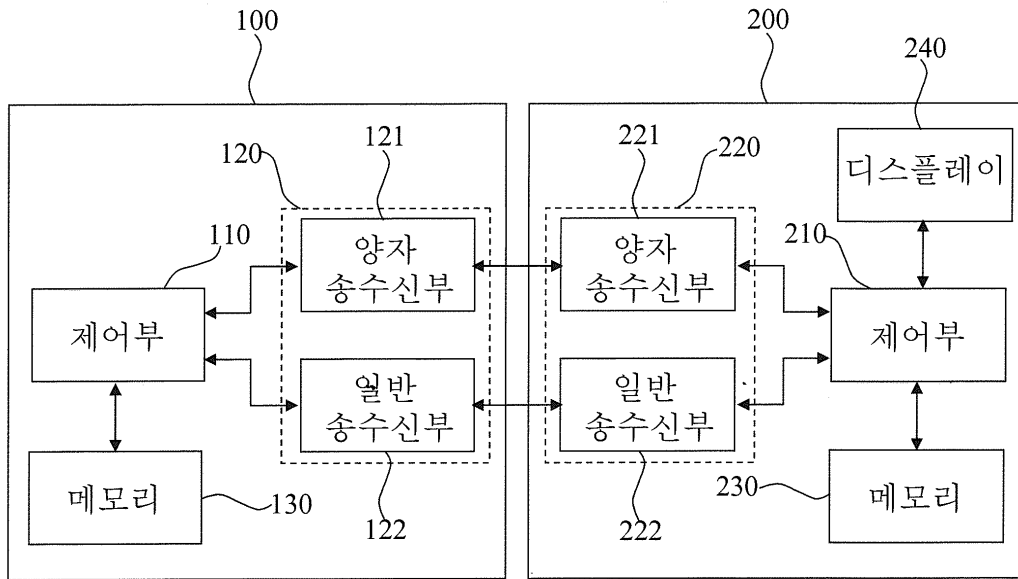
[0096] 100: 제1 기기 200: 제2 기기
110, 210: 제어부 120, 220: 송수신부
130, 230: 메모리

도면

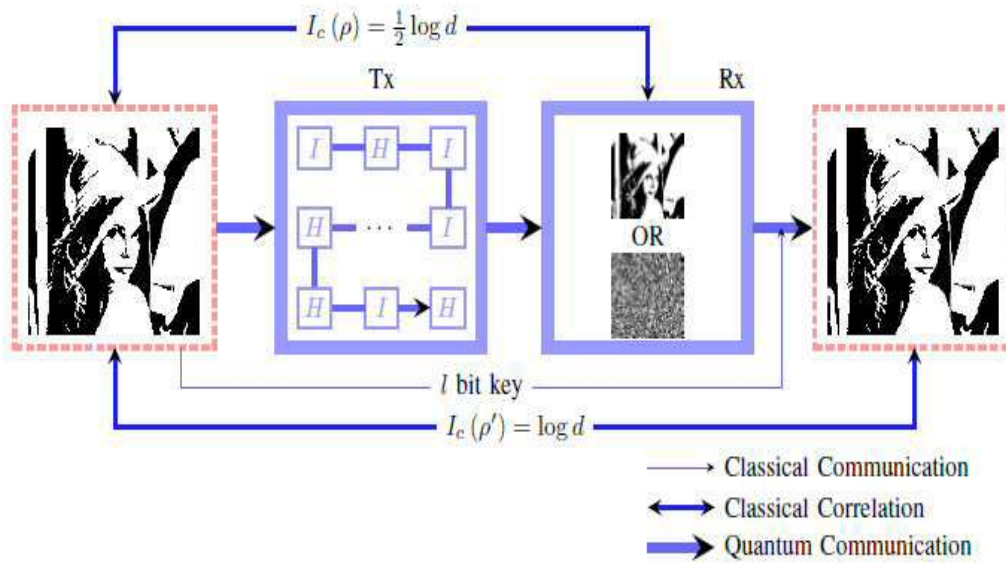
도면1



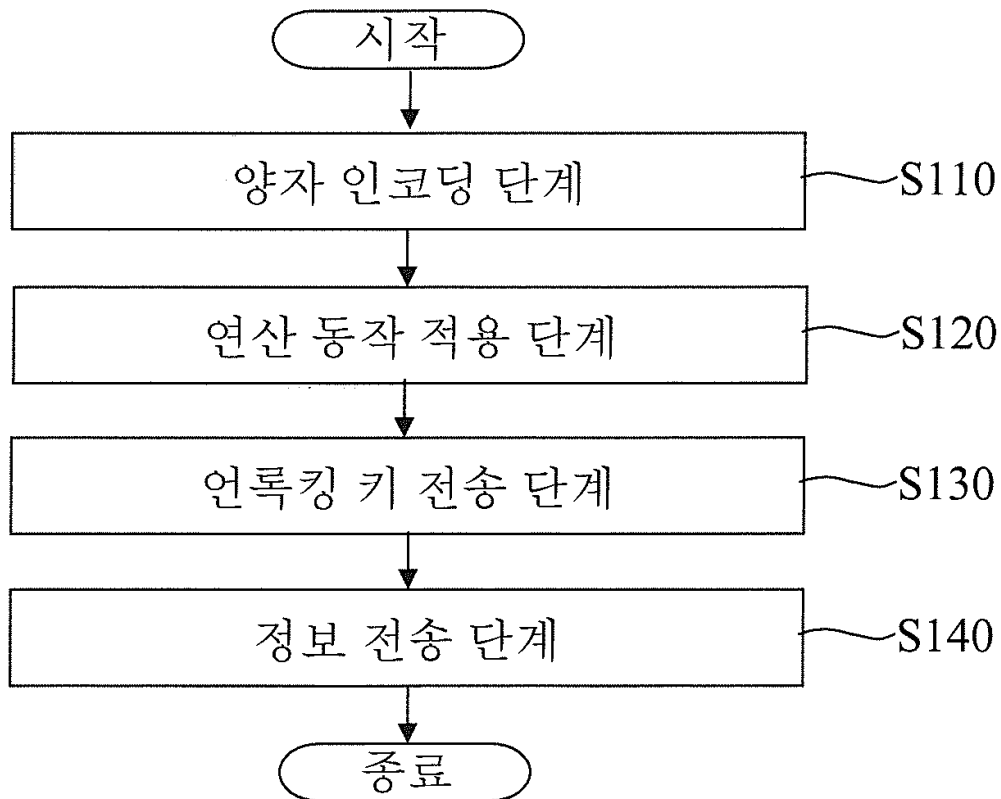
도면2



도면3



도면4



도면5

