양자직접통신 기술의 개요

박주윤, 허준*

고려대학교

{pjy1343, *junheo}@korea.ac.kr

요 약

본 논문은 최근 주목 받고있는 양자통신 기술 중 하나인 양자직접통신의 방법을 소개한다. 양자키분배 기술과 달리 송신자가 보내려는 정보를 양자상태에 직접 실어서 전송할 수 있는 원리를 설명하고 간단한 예시를 제시한다.

Ⅰ. 서 론

양자통신은 크게 양자키분배(Quantum Key Distribution)와[1] 양자직접통신(Quantum Secure Direct Communication)으로[2] 나뉜다. 두 기술 모두 양자상태의 복제불가능성을 기반하여 안전성을 보장받지만 큰 차이점이 존재한다. 양자키분배는 송신자와 수신자가 공통의 비밀키를 나눠갖고 이를 통해 보내고자 하는 정보를 암호화하는데 반해, 양자직접통신은 보내려는 정보를 직접 양자상태에 실어서 수신자에게 전송한다. 본 논문에서는 [3]에 기반하여 양자직접통신을 소개한다.

Ⅱ. 본론

송신자 Alice와 수신자 Bob이 통신을 할 때 두 개의 측정 기저가 필요하다. 하나는 십자 기저 $\{|H\rangle=|0\rangle, |V\rangle=|1\rangle\}$, 나머지 하나는 대각 기저로 다음과 같다.

$$\left\{|u\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle), |d\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\right\}$$

이 때, $|H\rangle$와 $|u\rangle$는 이진수 0, $|V\rangle$와 $|d\rangle$는 이진수 1을 의미한다.

양자직접통신은 두 개의 단계로 이뤄지는데 단계 1은 Bob이 Alice에게 양자상태를 전송하고 단계 2는 Alice가 Bob에게 받은 양자상태 중 일부를 다시 Bob에게 전송하는 단계로 자세한 과정은 다음과 같다.

단계 1 : Bob은 편광코딩된 단일광자들을 Alice에게 전송하고 이를 A-batch로 부른다. 이 때, 편광상태는 $\{|H\rangle, |V\rangle, |u\rangle, |d\rangle\}$ 중 하나이다. Alice는 수신한 광자들 중 일부를 골라서 이를 S-batch로 부르고 그 광자들을 임의로 기저로 측정한다. Alice는 Bob에게 S-batch의 위치와 측정 기저, 측정 결과를 공개하면 Bob은 Alice가 공개한 정보를 통해 오류율을 계산하고 도청 유무를 판단할 수 있다. Alice는 S-batch에 속하지 않은 A-batch 광자들을 B-batch로 정의한다.

단계 2 : Alice는 B-batch의 광자들에 정보를 입혀서 Bob에게 전송하는데 이 때 사용하는 두 개의 operator는 다음과 같다.

$$I=|0\rangle\langle 0|+|1\rangle\langle 1|,\ U=i\sigma_y=|0\rangle\langle 1|-|1\rangle\langle 0|$$

각각의 operator는 Alice가 보내려는 메시지 비트 0과 1에 해당하고 operator U를 통해 encoding되는 양자상태는 다음과 같다.

$$U|0\rangle=-|1\rangle,\ U|1\rangle=0,\ U|u\rangle=|d\rangle,\ U|d\rangle=-|u\rangle$$

A-batch가 Bob에 의해 준비되었기 때문에 Bob은 측정 기저와 Alice의 encoding 전 원래 양자상태를 알고 있다. Bob은 A-batch를 준비할 때 사용했던 basis를 이용하여 B-batch의 광자들을 측정하고 Alice가 전송한 비밀정보를 바로 읽어낸다. 보안성을 보장하기 위해서 Alice는 B-batch 중 일부의 비밀정보를 공개하고 Bob은 공개된 정보를 통해 도청의 유무를 확인할 수 있다.

그림 1은 앞서 설명한 양자직접통신의 간단한 예시이다. Bob은 Alice에게 A-batch를 보내면 Alice가 S-batch를 선정하여 측정결과를 Bob에게 보낸다. Alice와 Bob이 QBER에 이상이 없음을 확인하면 Alice는 남은 B-batch를 보내려는 정보에 기반한 operator로 encoding하여 Bob에게 전송한다. Bob은 A-batch 준비에 사용한 기저를 이용하여 수신 state 측정을 하고 A-batch와 측정값이 같은 경우 0, 다른 경우 1 정보를 Alice가 전송한 것을 알 수 있다.

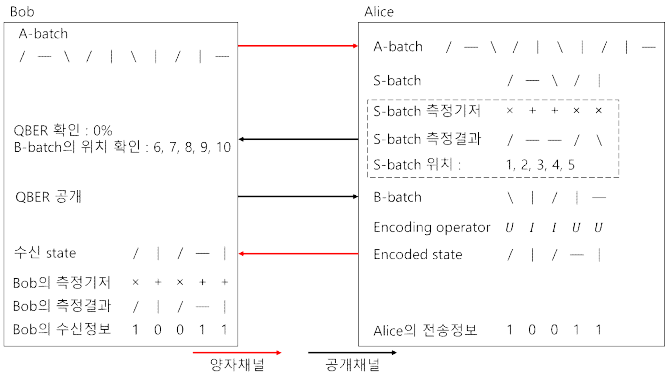

그림 1. 양자직접통신의 예시

Ⅲ. 결론

본 논문에서는 양자통신 기술 중 하나인 양자직접통신의 방법을 소개한다. 양자직접통신은 양자키분배 기술과 달리 송신자가 보내려는 정보를 양자상태에 직접 실어서 전송할 수 있고 양자역학의 성질에 의하여 절대적인 안전성을 보장하는 통신 기술이다.

ACKNOWLEDGMENT

본 연구 논문은 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No. 2020-0-00014, 결함허용 논리양자 큐빗 환경을 제공하는 양자운영체제 원천기술 개발)

참 고 문 헌

[1] C. H. Bennett and G. Brassard, Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing (IEEE, New York, 1984), pp. 175 - 179.

[2] Beige, Almut & Englert, Berthold-Georg & Kurtsiefer, Christian & Weinfurter, Harald. (2001). Secure Communication with a Publicly Known Key. Acta Physica Polonica A. 101.

[3] Deng, Fu-Guo, and Gui Lu Long. "Secure direct communication with a quantum one-time pad." Physical Review A 69.5 (2004): 052319.