# WDM channel에 따른 CV QKD 신호 분석

윤승호, 배성현, 허준*
고려대학교, 세종대학교, *고려대학교
seunghoyoon@korea.ac.kr, sungbae@sejong.ac.kr, *junho@korea.ac.kr

**Analysis of CV-QKD Signals under WDM Channels**

Seungho Yoon, Sunghyun Bae, Heo Jun*
Korea Univ., Sejong Univ, *Korea Univ.

**요 약**

본 논문은 WDM 환경에서 채널 수가 증가할 때 CV-QKD 신호 성능에 미치는 영향을 정량적으로 분석하고, 그 결과가 실용적 시스템 설계에 갖는 함의를 논의한다. 후속 연구로는 본 연구에서 축적한 데이터셋을 활용하여 신호 복구 및 잡음 보정을 수행하는 후처리 알고리즘을 개발하는것이 필수적이다.

## 1. 서론

양자키 분배 기법은 보안성관련하여 많은 주목을 받고 있는 분야이다. 양자 키 분배(QKD)는 단일 광자에 정보를 부호화해 전송하고, 공개 채널을 통해 송신자와 수신자가 비밀 키를 합의하는 기술로, 도청자가 개입하면 그 흔적을 검출할 수 있다. 일반적으로 송신자(앨리스)가 단일 광자의 양자상태에 정보를 부호화해 수신자(밥)에게 전송하면, 만약 도청자(이브)가 측정 · 가로채기를 시도할 경우 오류율이 상승하는 등 교란이 발생하여 그 존재를 확인할 수 있다[1].

대표적인 양자 키 분배 프로토콜로 BB84가 있다. 이론적으로 BB84는 단일 광자를 생성해 수신자에게 전송하는 과정을 전제로 하며, 이는 단일 광자를 복제할 수 없다는 no-cloning theorem 에 기반한다. BB84에서는 비트 값 0과 1을 표현하기 위해 수직/수평(H/V) 기저와 대각 기저를 사용한다. H/V 기저에서는 0°와 90°가 각각 비트 0과 1에 대응하고, 대각 기저에서는 45°와 135°가 비트 0과 1을 나타낸다고 볼 수 있다. 이후 절차는 그림 1과 같이 송신자와 수신자가 공개 채널을 통해 일부 정보를 공개 · 비교하는 단계로 이어진다.

그러나 실제 구현에서는 송신자(앨리스)가 레이저 펄스를 발생시킨 뒤 감쇄하여 단일 광자 상태를 만들며, 이때 단일 광자가 생성될 확률뿐 아니라 다중 광자가 생성될 확률도 존재한다. 이러한 한계를 보완하기 위한 접근으로 연속변수(Continuous Variable, CV) QKD가 개발되었다[2]-[5].

## 2. 본론

CV QKD 시스템 구현은 아래와 같은 다이어그램을 통해서 구현을 진행하였음.

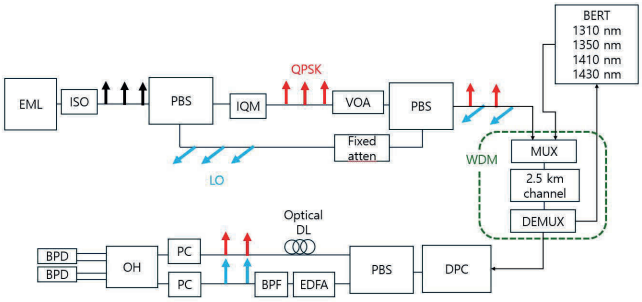


Figure 1: CV QKD 구현 다이어그램

EML laser로 pulsed laser를 생성 후, PBS를 통해 upper path, lower path로 분리하였음. 이후 upper path의 pulse에 QPSK 신호를 인코딩 하고, lower path는 LO 신호로써 사용하였음. 이후 PBS를 통해 time bin PDM 으로 신호를 WDM 장비로 전송하였음. WDM 장비는 1310, 1350, 1410, 1430 nm 파장대역의 OOK 신호가 함께 mux 되어있음

2.5 km channel이 없을때의 constellation 과 2.5 km channel이 존재할 때의 constellation을 비교하기 위해 데이터 추출을 진행하였음.

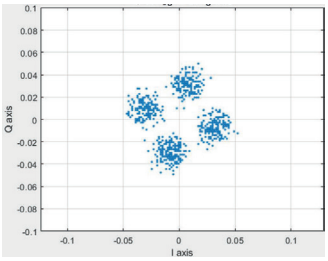


Figure 2: no 2.5 km channel constellation

위 그림은 WDM-QKD 시스템에 2.5 km channel 이 없을때의 constellation이다.

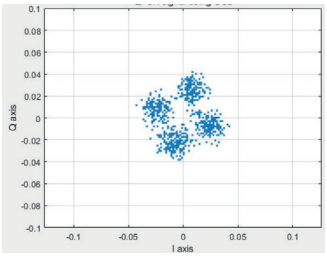


Figure 3: 2.5 km channel constellation

위 그림은 WDM-QKD 시스템에 2.5 km channel 이 존재할 때의 constellation이다.

가시작으로 channel이 늘어남에 따라 constellation 의 amplitude가 감소했음을 확인하였다. 추가로 symbol error 율도, channel 추가 전에는 0 % 였지만 2.5 km channel 추가 후에는 symbol 오류율이 약 1.2 % 로 증가하였음을 확인하였다.

## 3. 결론

본 논문은 CV QKD가 1310, 1350, 1410, 1430 nm 파장대역의 신호와 함께 muxing되었을 때의 신호분석을 확인하였다. Muxing이후 정상적인 constellation 이 추출되었으며 symbol 오류율도 1.2 %로 매우 미미하게 영향을 받은것을 확인 할 수 있었다.

## ACKNOWLEDGMENT

이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. RS-2023-00242396).

본 연구는 한국과학기술정보연구원(KISTI)의 위탁연구개발과제로 수행한 것입니다.

이 논문은 정부(과학기술정보통신부)의 재원으로 한국연구재단 양자정보과학 인적기반 조성사업의 지원을 받아 수행된 연구임 (Grant No. 2022M3H3A1063074).

## 참 고 문 헌

1. Jain, Nitin, et al. “Practical continuous-variable quantum key distribution with composable security.” *Nature communications* 13.1 (2022): 4740.

2. Ralph, Timothy C. “Continuous variable quantum cryptography.” *Physical Review A* 61.1 (1999): 010303.

3. Grosshans, Frédéric, and Philippe Grangier. “Continuous variable quantum cryptography using coherent states.” *Physical Review Letters* 88.5 (2002): 057902.

4. Zhao, Huanxi, et al. “Simple continuous-variable quantum key distribution scheme using a Sagnac-based Gaussian modulator.” *Optics Letters* 47.12 (2022): 2938–2942.

5. Roussel, François, et al. “Demonstration of probabilistic constellation shaping for continuous variable quantum key distribution.” *Optical Fiber Communication Conference*. Optica Publishing Group, 2021.