WDM-QKD 시스템을 위한 CV QKD 구현 및 후처리 기법

윤승호, 허준*
고려대학교, *고려대학교
seunghoyoon@korea.ac.kr, *junho@korea.ac.kr

Implementation and Post-Processing Techniques of CV-QKD for WDM-QKD Systems

Seungho Yoon, Heo Jun*
Korea Univ., *Korea Univ.

요 약

본 논문은 연속 변수 양자 암호키 분배(continuous variable quantum key distribution)의 최근 기술 연구 동향을 분석하는 논문이다. 특히 CV QKD가 optical amplifier(광 증폭기)를 거친 이후 어떤 후처리가 필요한지 이론적 분석과 시뮬레이션 결과를 통해 검토한다. 후속 연구 방향으로는 신호 복구 및 잡음 보정을 위한 후처리 알고리즘에 대한 고찰이 필요하다.

1. 서론

CV QKD(Continuous-Variable Quantum Key Distribution)는 광자의 진폭과 위상과 같은 연속적인 물리량을 이용하여 비밀 키를 공유하는 양자 키 분배 방식이다[1]. 기존의 이산 변수 QKD(DV QKD)와 달리, CV QKD는 상용 통신 시스템에서 사용되는 코히런트 광원 및 고속 동조 검출기(homodyne, heterodyne detection)를 기반으로 하므로, 기존 광통신 인프라와의 호환성이 높고 구현이 용이하다는 장점이 있다[2]. 특히 고속 전송과 집적화된 회로 환경에서의 운용이 유리하여, 대규모 네트워크 통합을 위한 유망한 QKD 구현 기술로 주목받고 있다.

2. 본론

CV QKD 기법에서는 전송자가 QKD, LO 신호 두 개를 전송해야된다[3][4]. 가장 기본적인 형태의 CV QKD는 전송자인 Alice가 QKD, LO 신호를 동시에 전송하는 형태이다[5].

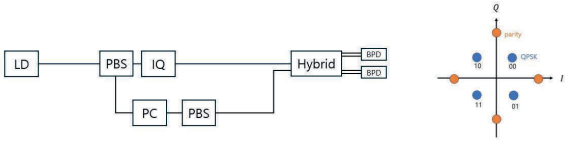

Figure 1: (좌)기본적인 CV QKD 다이어그램 (우)Encoded signal

그러나 이러한 형태는 WDM과의 병합이 어렵다. WDM 장비에는 경우에 따라 특정 파장대역의 port가 1개뿐인 경우도 있기 때문이다. 이럴 경우 QKD 신호와, LO 신호를 병합하여 하나의 optical fiber로 전송하는 기법이 필요하다. 이를 위해서 polarization mutliplexing 기법을 사용하여 아래와 같은 다이어그램의 CV QKD를 구현하였다.

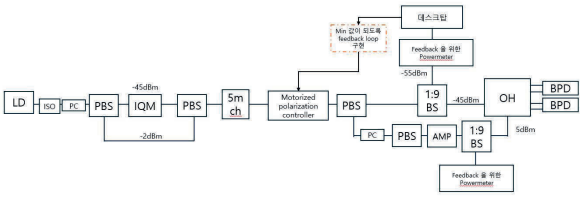

Figure 2: Polarization multiplexed CV QKD

이 시스템에서 추출한 raw data는 아래와 같이 나왔다. 이 raw data의 일부를 추출하여 확인해보면 data가 원점에서 조금 벗어난 형태로 phase noise의 영향을 받고 있는것을 볼 수 있다. 이는 QKD 신호에 LO 신호가 미세하게 혼합되어 들어갔기 때문이다. 이러한 이유로, raw data를 원점으로의 조정이 필요하였다.

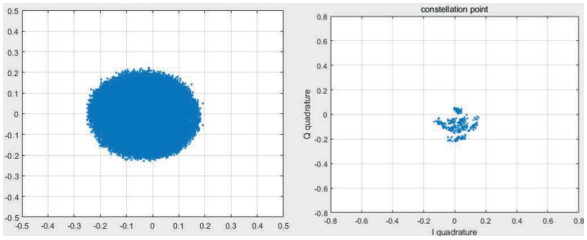

Figure 3: (좌)raw data (우)raw data의 일부

Raw data를 원점으로 조정 후, 각 symbol들의 sample의 mean 값으로 후처리 후 parity 신호를 활용하여 phase noise를 보상하였다.

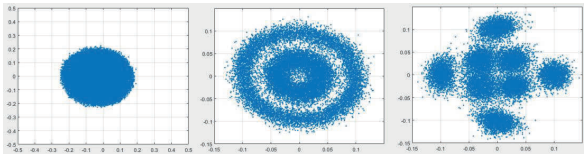

Figure 4: (좌)raw data (중)원점으로 조정 (우) phase noise 보상

이때의 QBER 값은 11.38 % 이다. 이러한 높은 QBER을 극복하고자 weight mean 기법으로 symbol들의 sample 후처리를 진행하였다. 총 5개의 symbol의 weight는 [0, 0.2, 0.4, 0.4, 0] 로 설정하고 위와 같은 후처리를 진행하였다. 이에 대한 결과로 QBER이 6.68 %로 낮아지는것을 확인하였다.

3. 결론

본 논문은 CV QKD가 optical amplifier(광 증폭기)를 거친 이후 어떤 후처리가 필요한지 이론적 분석과 시뮬레이션 결과를 검토하였다. 데이터 후처리 과정에서 symbol들을 mean 으로 통합하여 후처리를 진행하는것 보다, 최적화된 값의 weighted mean을 진행하는것이 더욱 높은 성능의 QBER을 보이는것을 확인하였다.

ACKNOWLEDGMENT

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

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

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.