

Transmitted Lo CV QKD 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.

요약

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

Transmitted LO 기반의 CV QKD는 로컬 오실레이터(LO)를 송신자가 생성하여 전송하는 구조를 취함으로써 수신 측의 보안성과 시스템 단순화를 동시에 추구한다. 하지만 이 구조는 optical amplifier와 같은 실험 구성 요소로 인해 LO 신호가 QKD 신호와 섞이는 위상 잡음(phase noise) 문제가 존재하며, 이에 대한 후처리 보정 기술이 필수적이다.

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].

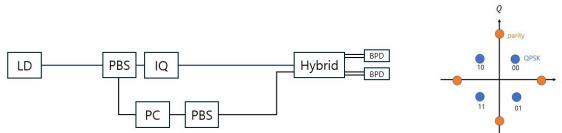


Figure 1: (좌)기본적인 CV QKD 다이어그램 (우)Encoded signal

그러나 이러한 형태는 현실적인 구현 관점에서 어려운 부분이 있다. 두개의 optical fiber가 전송 channel을 지나게되면 도청자의 개입이 더욱 쉬워지기 때문이다. 이러한 현상을 방지하고자 QKD 신호와, LO

신호를 병합하여 하나의 optical fiber로 전송하는 기법이 필요하다. 이를 위해서 polarization multiplexing 기법을 사용하여 아래와 같은 다이어그램의 CV QKD를 구현하였다.

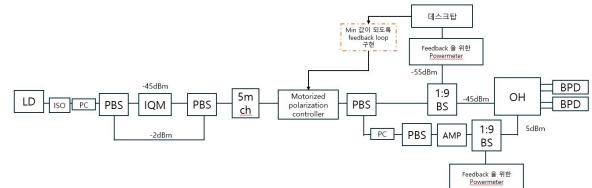


Figure 2: Polarization multiplexed CV QKD

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.

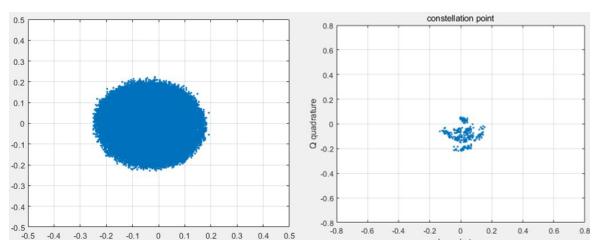


Figure 3: (좌)raw data (우)raw data의 일부

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

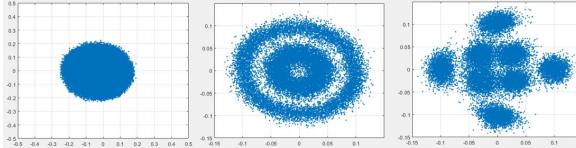


Figure 4: (좌)raw data (중)원점으로 조정 (우) phase noise 보상

이때의 QBER 값은 11.38 % 이다.

3. 결론

본 논문은 CV QKD가 optical amplifier(광 증폭기)를 거친 이후 어떤 후처리가 필요한지 이론적 분석과 시뮬레이션 결과를 검토하였다. 향후 연구는 CV QKD 수준의 optical power로 낮춰서 동일한 실험을 진행하는것이 예정되어있다.

ACKNOWLEDGMENT

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

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.