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

e ng o oon eo n
orea niv orea niv

요 약

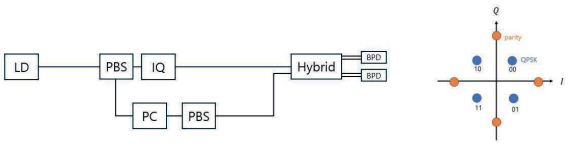
본 논문은 연속 변수 양자 암호키 분배(con in o s variable an m ke dis rib ion)의 최근 기술 연구 동향을 분석하는 논문이다 특히 C D가 o ical am li er(광 증폭기)를 거친 이후 어떤 후처리가 필요한지 이론적 분석과 시뮬레이션 결과를 통해 검토한다 후속 연구 방향으로는 신호 복구 및 잡음 보정을 위한 후처리 알고리즘에 대한 고찰이 필요하다

1. 서론

Transmi ed 기반의 C D는 로컬 오실레이터( )를 송신자가 생성하여 전송하는 구조를 취함으로써 수신 측의 보안성과 시스템 단순화를 동시에 추구한다 하지만 이 구조는 o ical am li er와 같은 실험 구성 요소로 인해 신호가 D 신호와 섞이는 위상 잡음(ase noise) 문제가 존재하며 이에 대한 후처리 보정 기술이 필수적이다

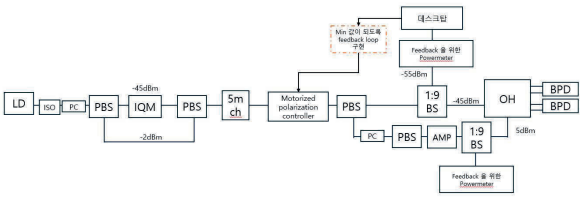
2. 본론

C D 기법에서는 전송자가 D 신호 두 개를 전송해야된다[3][4] 가장 기본적인 형태의 C D는 전송자인 lice가 D 신호를 동시에 전송하는 형태이다[5]



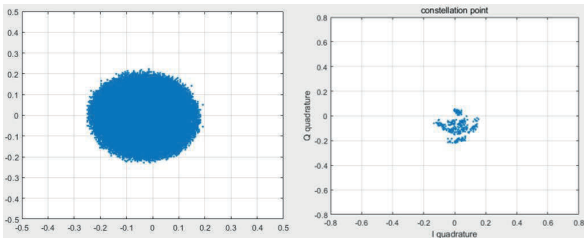
ig re 1 (좌)기본적인 C D 다이어그램 (우) ncoded signal

그러나 이러한 형태는 현실적인 구현 관점에서 어려운 부분이 있다 두개의 o ical ber가 전송 c an nel을 지나게되면 도청자의 개입이 더욱 쉬워지기 때문이다 이러한 현상을 방지하고자 D 신호와 신호를 병합하여 하나의 o ical ber로 전송하는 기법이 필요하다 이를 위해서 olari a ion m li lex ing 기법을 사용하여 아래와 같은 다이어그램의 C D를 구현하였다



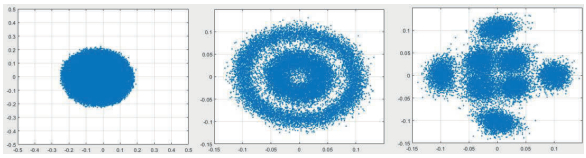
ig re 2 Polari a ion m l i lexed C D

이 시스템에서 추출한 ra da a는 아래와 같이 나왔다 이 ra da a의 일부를 추출하여 확인해보면 da a가 원점에서 조금 벗어난 형태로 ase noise의 영향을 받고 있는것을 볼 수 있다 이는 D 신호에 신호가 미세하게 혼합되어 들어갔기 때문이다 이러한 이유로 ra da a를 원점으로의 조정이 필요하였다



ig re 3 (좌)ra da a (우)ra da a의 일부

a da a를 원점으로 조정 후 각 s mbol들의 sam le의 mean 값으로 후처리 후 ari 신호를 활용하여 ase noise를 보상하였다



ig re 4 (좌)ra da a (중)원점으로 조정 (우) ase noise 보상

이때의 값은 11 38 이다

3. 결론

본 논문은 C D가 o ical am li er(광 증폭기)를 거친 이후 어떤 후처리가 필요한지 이론적 분석과 시뮬레이션 결과를 검토하였다 향후 연구는 C D 수준의 o ical o er로 낮춰서 동일한 실험을 진행하는것이 예정되어있다

ACKNOWLEDGMENT

이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(o 2023 002423 6)

본 연구 논문은 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (o 2020 0 00014 결함허용 논리양자큐빗 환경을 제공하는 양자운영체제 원천기술 개발)

참 고 문 헌

1 ain i in e al Prac ical con in o s variable an m ke dis rib ion i com osable sec ri *Nature communications* 13 1 (2022) 4740

2 al Timo C Con in o s variable an m cr ogra *Physical Review A* 61 1 (1) 010303

3 ross ans rederic and P ili e rangier Con in o s variable an m cr ogra sing co eren s a es *Physical Review Letters* 88 5 (2002) 057 02

4 ao anxi e al im le con in o s variable an m ke dis rib ion sc eme sing a agnac based a ssian mod la or *Optics Letters* 47 12 (2022) 2 38 2 42

5 o ssel rancois e al Demons ra ion o robabilis ic cons ella ion s a ing or con in o s variable an m ke dis rib ion *Optical Fiber Communication Conference* ica P blis ing ro 2021