# CV-QKD를 위한 BPSK 기반 IQ 변조 시스템의 설계 및 분석에 관한 연구

이상규, 허 준*

고려대학교, *고려대학교

2023020754@korea.ac.kr, *junheo@korea.ac.kr

# A Study on the Design and Analysis of BPSK-Based IQ Modulation System for Continuous-Variable Quantum Key Distribution (CV-QKD)

Lee Sang Gyu, Heo Jun*

Korea Univ., *Korea Univ.

요 약

본 논문은 IQ-Modulator를 사용하여 이진 위상 변조(BPSK)에 기반한 Continuous Variables Quantum Key Distribution (CV-QKD)를 설계하고 분석하였다. IQ-Modulation의 I-axis 상에서 이진 위상 변조(BPSK)를 진행하고 검출된 신호를 오실로스코프를 사용하여 파형을 관측했다.
본 실험에서의 중점적으로 다루는 내용은 Digital Signal Processing (DSP)단계 이전의 신호 검출 단계이다. 각각의 소자의 동작 원리와 수식적인 해석으로 BPSK 기술을 사용하여 IQ 변조 시스템을 구현하는 과정과 실험 결과를 간결하게 소개하고 있다. 실험 결과로부터 Q-axis와 함께 변조를 진행하면 추후 Quadrature Amplitude Modulation(QAM) 기반한 CV-QKD에 대해 확장 가능성을 보였다.

## Ⅰ. 서 론

현대의 디지털 통신은 보안 문제에 직면하고 있으며, 전통적인 암호화 방법의 한계를 경험하고 있다. 양자 통신은 양자역학의 원리를 활용하여 정보를 보호하는 혁신적인 방법을 제공하며, 보안 통신 시스템의 핵심 요소로 여겨지고 있다. CV-QKD는 연속 변수 양자 시스템을 기반으로 하며, 빛의 진폭과 위상을 이용하여 안전한 키 분배를 실현할 수 있는 기술이다. 단일광자광원과 단일광자검출기를 사용하지 않고 QKD를 할 수 있는 방법을 연속변수(Continuous Variable, CV) 기반 QKD라고 한다. CV-QKD는 빛 즉 전자기장의 퀴드러처(Quadrature)라는 연속적인 변수 특성으로 암호화하고 코히어런트 검출(Coherent Detection)이라는 고전 광 검출 기술로 복호화하여 비밀키를 만들어낸다. 코히어런트 검출기는 단일광자검출기와 달리 별도의 냉각 과정 없이도 높은 검출 효율(90%)을 보이고, 현존하는 광통신 장치들과의 호환성이 좋기 때문에 기존 단일광자 검출기보다 실용적이다.

CV-QKD의 장점은 기존의 고전 광통신 기술을 이용해 구현할 수 있다는 점뿐만 아니라, 단일 모드 필터 역할을 국부 진동자(Local Oscillator, LO)특성 덕분에 배경잡음의 영향을 잘 받지 않는다. 하지만 높은 키 생성률을 위해서는 저잡음 검출기, 효율적인 오류정정 코드, 정확한 매개변수 추정 등의 기술이 더 필요하고, 도청 공격에 대한 보안성 증명도 해결해야할 과제로 남아있다.

본 실험에서는 IQ-Modulator를 사용하여 이진 위상 변조(BPSK)에 기반한 Continuous Variables Quantum Key Distribution (CV-QKD)를 설계하고 분석하였다. BPSK(Binary Phase Shift Keying)는 디지털 통신에서 사용되는 이진 위상 변조 기술 중 하나이다. BPSK는 이진 데이터를 변조하여 전송하는 방식으로, 각 비트를 두 가지 상태의 위상으로 표현한다. 우리는 IQ-Modulator를 사용하여 I-axis 상에 binary 데이터를 $0$과 $\pi$에 인코딩(encoding)하여 BPSK를 구현하였다. CV-QKD의 시스템에 있어서 각각의 소자의 동작 원리와 수식적인 해석으로 BPSK 기술을 사용하여 IQ 변조 시스템을 구현하는 과정과 실험 결과를 간결하게 소개하려고 한다.

## Ⅱ. 본론

### A. Experimental Setup

본 실험의 setup은 그림 1에 보여지고 있다. 먼저 송신단(Alice)에 대한 설명이다. 1550nm의 CW 레이저를 사용하여 광원을 생성하고 9:1 BS(Beam Splitter)를 사용하여 LO 신호와 QKD 신호로 사용할 광원을 분리한다. 다음 QKD 광원은 IQ-Modulator를 통해 I-axis의 BPSK 변조를 진행한다. 수신단(Bob)에서는 먼저 $90^\circ$ Optical Hybrid의 입력으로 수신된 QKD 신호와 LO 신호를 받고 출력으로 $(S+L),(S-L)$의 광신호를 내보낸다. 사실 $90^\circ$ Optical Hybrid는 IQ 변조 된 신호를 검출하기 위해 사용되는데 우리는 I-axis 상의 신호만 확인하기 때문에 2개의 출력만 사용한다. 나머지 2개의 출력 $(S+jL),(S-jL)$은 Q-axis 상의 신호를 검출하기 위해 사용된다. 다시 이렇게 출력된 $(S+L),(S-L)$ 신호는 Balanced Photo Detector(BPD)의 입력으로 들어가서 최종 I-axis 상의 데이터를 추출하여 Oscilloscope(OSC)에 파형을 출력한다.

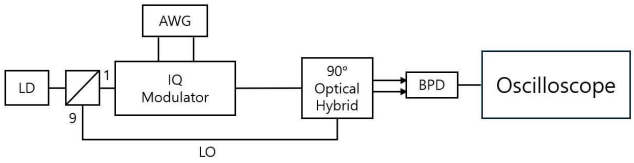


그림 1 : Experimental Setup

### B. IQ 변조기 (IQ-Modulator)

IQ 변조기는 임의 파형 발생기(AWG)를 통해 인코딩 하려는 신호를 인가하여 transfer function 과 만나 IQ 변조를 진행한다. 이 때 IQ 변조기의 bias voltage는 null point로 맞춰준다. null point로 설정하는 이유는 입력신호를 가장 왜곡 없이 출력하는 지점이다. 또한 transfer function을 통한 encoding을 더욱 효율적으로 진행하기 위함이다 .아래의 그림은 null point에서의 IQ 변조 과정을 보여준다.

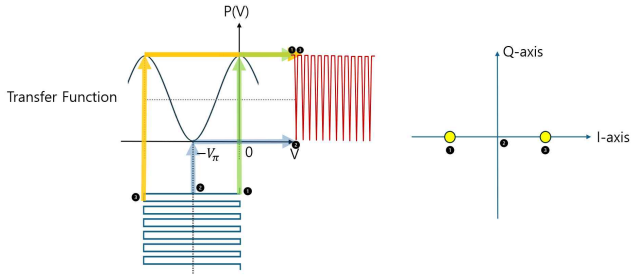


그림 2 : Null point에서의 transfer function 동작 과정

### C. 헤테로다인 검출기(Heterodyne Detector)(90 ° Optical Hybrid , Balanced Photo Detector)

다음은 헤테로다인 검출기(Heterodyne Detector)의 수식적인 동작 원리에 대해 설명한다. IQ-Modulator의 목적은 I-axis와 Q-axis 상의 정보를 인코딩하기 위함이다 따라서 헤테로다인 검출기를 사용해 I-data와 Q-data를 한 번에 추출하게 된다. 하지만 위의 실험에서는 I-axis 상의 정보만을 필요로 하기 때문에 호모다인 검출기(Homodyne Detector)로 구성하였다. 호모다인 검출기와 헤테로다인 검출기의 차이점은 동시에 I-axis와 Q-axis의 data를 동시에 추출할 수 있는지 없는지로 결정이 된다. 하나의 축의 데이터만 추출하면 호모다인 검출기, 두 개의 축의 데이터를 동시에 추출 가능하면 헤테로다인 검출기이다. 헤테로다인 검출기는 90 ° Optical Hybrid와 Balanced Photo Detector로 구성되어있다.

90 ° Optical Hybrid는 2개의 입력신호 S와 L을 받아 Phase shifter를 통해 I-axis 데이터와 Q-axis 데이터 추출에 필요한 위상을 변환하여 4개의 출력 $(S+L),(S-L)$ 과 $(S+jL),(S-jL)$를 내보낸다. BPD의 역할은 두 개의 신호의 차이를 출력한다. 이 때 공통모드잡음을 제거하고 신호의 크기를 증폭 해준다. 아래의 수식에서 L은 LO 신호를 의미하고 S는 QKD 신호를 의미한다. 여기서 L은 변조되지 않은 신호이므로 상수 취급하였다.

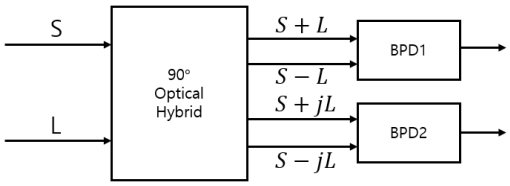


그림 3 : Heterodyne Detector

BPD1 output : I-Data

$$(S+L)(S+L)^* - (S-L)(S-L)^*$$
$$= (SS^* + SL^* + LS^* + LL^*) - (SS^* - SL^* - LS^* + LL^*)$$
$$= 2SL^* + 2LS^*$$
$$= 2(S+S^*)$$

BPD2 output : Q-Data

$$(S+jL)(S+jL)^* - (S-jL)(S-jL)^*$$
$$= (SS^* - jSL^* + jLS^* + LL^*) - (SS^* + jSL^* - jLS^* + LL^*)$$
$$= -2jSL^* + 2jLS^*$$
$$= -2j(S-S^*)$$

### D. 실험 결과

본 실험에서는 IQ-Modulator를 사용하여 BPSK를 구현하였다. 따라서 IQ-plane에서 I-axis 상에 두 constellation point$(0\ ,\pi)$에 인코딩을 했으며, 그림 1에서 볼 수 있듯이 본 실험은 BPD를 통해 QKD 신호를 검출했다. 그래프의 양의 peak 값은 비트 값 1에 mapping되고 음의 peak 값은 비트 값 0에 mapping된다. 신호의 속도는 AWG에서 50MHz로 설정하였으며 비트 값 1과 0이 반복되도록 설정하였다.

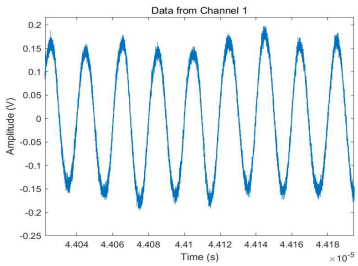


그림 4 : I-axis의 BPD 출력

## Ⅲ. 결론

본 논문에서는 IQ-Modulator를 사용하여 이진 위상 변조(BPSK)에 기반한 Continuous Variables Quantum Key Distribution (CV-QKD) 시스템을 설계하고 분석하였다. 본 연구에서는 I-axis 상에서 BPSK 변조를 성공적으로 수행하여 CV-QKD 시스템에 적용하였다. 송신단에서 1550nm CW 레이저와 9:1 빔 스플리터를 이용하여 LO 신호와 QKD 신호를 분리하고, IQ-Modulator를 통해 BPSK 변조를 진행하였다. 수신단에서는 Optical Hybrid와 BPD를 사용하여 I-axis 신호를 검출하였다. 검출된 신호를 오실로스코프를 통해 파형으로 관측하여 BPSK 신호의 양의 피크 값이 비트 값 1, 음의 피크 값이 비트 값 0으로 mapping되는 것을 확인하였다.


## ACKNOWLEDGMENT

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터육성지원사업의 연구결과로 수행되었음 (IITP-2024-2021-0-01810)

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


## 참 고 문 헌


[5]Roumestan, Francois, et al. "Shaped Constellation Continuous Variable Quantum Key Distribution: Concepts, Methods and Experimental Validation." Journal of Lightwave Technology (2024).