구현 시스템 최적화를 통한 CV-QKD 신호 측정 및 후처리

윤승호, 배성현, 김범일, 김성욱, 허준*

고려대학교, 강원대학교, *고려대학교

seunghyoon@korea.ac.kr, baesh@kangwon.ac.kr, *junheo@korea.ac.kr

MeasurementandPost-ProcessingofCV-QKDSignalsThroughImplementationSystem Optimization

Seungho Yoon, Sunghyun Bae, Heo Jun*

Korea Univ., Kangwon Nat Univ., *Korea Univ.

요 약

본 논문은 연속 변수 양자 암호키 분배(continuous variable quantum key distribution) 기법의 구현을 진행하였다. 구현에 필요한 시스템 최적화 방법을 기술하여 매우 낮은 optical power의 CV QKD 가 정상적으로 측정이 되도록 그 방법론을 확인하였으며, 본 CV QKD 신호의 후처리 과정을 보이도록 한다.

Ⅰ. 서 론

양자 키 분배(Quantum Key Distribution, QKD)는 양자역학적 특성을 이용해 통신 당사자 간에 비밀키를 생성·분배하는 방법으로, 양자 암호통신 분야에서 핵심적인 기술로 널리 연구되고 있다. 일반적으로 QKD는 사용되는 물리량에 따라 이산변수 방식(DV-QKD)과 연속변수 방식(CV-QKD)으로 구분된다. DV-QKD는 단일광자 수준에서 편광이나 위상과 같은 이산적인 상태를 정보를 담는 데 활용하는 반면, CV-QKD는 빛의 연속적인 정보를 실어 전송한다.[1].

CV-QKD는 기존 광통신 기술과의 친화성이 높다는 점에서 주목된다. 즉, 일반적인 광섬유 기반 통신망에 이미 널리 보급된 표준 부품 및 시스템 구조를 기반으로 구현이 가능하며, 단일광자 수준의 검출을 요구하는 방식과 달리 고가의 단일광자 검출기 없이도 수신이 가능하다. 대신 PIN 포토다이오드나 밸런스드 포토디텍터(Balanced Photodetector, BPD)처럼 상용화되어 접근성이 높은 검출기를 활용할 수 있어 비용 및 시스템 복잡도 측면에서 이점을 갖는다[2 - 4].

Ⅱ. 본론

본 논문에서 구현한 CV QKD 시스템은 아래와 같다. EML 레이저를 통해서 pulse laser를 생성하고 이후 Isolator 소자를 통해서 빛의 안정화를 진행한다. 이후 polarization beam splitter를 통해서 편광 분리를 하고, 위쪽 경로는 IQ modulator(IQM)을 사용해서 QKD encoding을 진행하고 아래쪽 경로는 local oscillator(LO)로써 사용하게 된다. 위쪽 경로에 있는 1:9 beam splitter를 통한 monitor 는, 편광의 안정화를 확인하기 위해 monitor 신호로 사용하였다. 이후 QPSK 신호는 variable optical attenuator를 사용하여, QKD level 까지 attenuation을 진행하게 된다.

아래 경로의 LO 신호는, EDFA를 통해서 증폭을 해주고, Bandpassfilter를 통해서 ASE noise를 제거해주게 된다. 이후 VOA를 통해서 목표 LO optical power로 설정하게 된다. 1:9 BS는, 위쪽 경로와 동일하게 신호의 안정화를 위해 monitor 신호를 확인하게 된다.

전송된 신호는 Bob이 polarization controller(PC)를 사용해서 수신하게 된다. 이후 OH의 output으로 S+L, S-L, S+iL, S-iL 의 신호가 나오게 된다. 이 4개의 신호들중 S+L, S-L은 하나의 BPD로 들어가서 I축의 데이터를 measure하게 되고, S+iL, S-iL 의 신호는 또 다른 BPD로 들어가서 Q축의 데이터를 measure하게 된다.

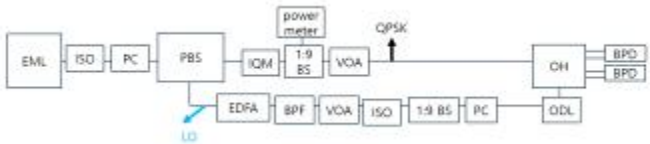

그림1. 구현한 CV QKD 시스템 다이어그램

구현한 시스템에서 매우 작은 신호인 CV-QKD 신호를 측정하기에 앞서, 시스템의 전반적인 최적화를 진행할 필요가 있다. 사용하는 BPD는 thorlab 사의 PDB425C 제품으로, 본 제품의 LO input 대비 shot noise response를 확인하여 CV-QKD에 사용할 최적의 LO-power를 확인하였다.

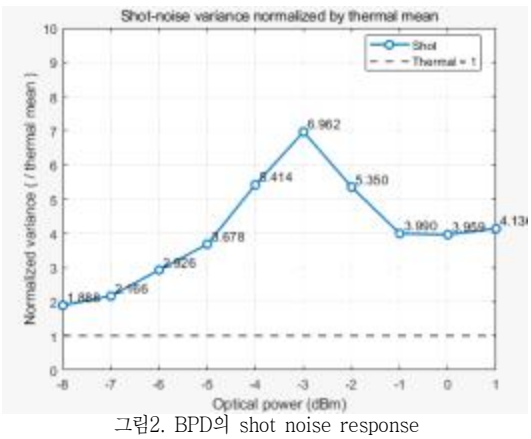

그림2. BPD의 shot noise response

그림 2를 확인하면 LO optical power -3 dBm에서 가장 높은 response를 보이는 것을 확인할 수 있다. 그 이상은 오히려 response가 떨어지기 때문에 CV-QKD 시스템에서 LO power는 -4 ~ -3 dBm으로 진행을 하

였다. 추가로 구현한 시스템에서의 PC를 사용하여 오실로스코프상의 신호의 크기가 최대가 되도록 acquisition을 진행 후 데이터 추출을 하게 된다.

이렇한 방법을 사용하여 QKD 신호의 I,Q축의 데이터를 추출하게 된다. 추출한 데이터를 바탕으로 raw data의 constellation point를 찍어보면 그림 3과 같이 확인을 할 수 있다.

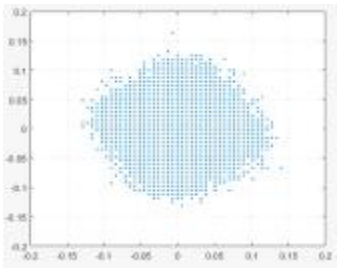

그림3. 추출한 raw data 의 constellation point

Raw data의 후처리를 진행하기 위해서는 phase noise compensation, lowpass filter, CMA 알고리즘을 거치게 된다. 이 DSP 과정을 통해서 inter symbol interference(ISI)를 제거하여 전송한 CV-QKD 신호를 명확하게 추출하는 과정을 진행하게 된다. Pulse와 encoding은 10 MBaud 로 진행이 되었기 때문에 LPF알고리즘도 이에 맞추어 후처리가 진행이 되었다.

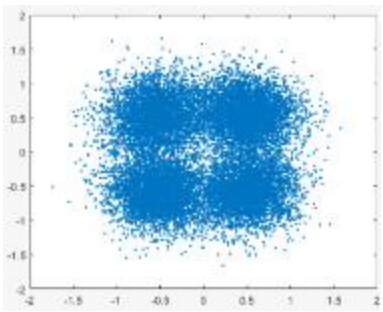

그림4. 후처리 진행한 후의 CV-QKD 신호

Ⅲ. 결론

CV QKD에서 신호를 추출 후 진행되는 DSP 처리 하는 방법을 확인하였다. CV QKD에서 후처리가 DV QKD보다 중요한 이유는, CV QKD가 연속 변수 신호를 활용하기 때문에 신호 품질에 영향을 미치는 여러 가지 요인에 더욱 민감하기 때문이다. CV QKD에서는 신호 검출 과정에서 잡음과 왜곡이 발생하기 쉽기 때문에 Parity 신호를 추가하면 데이터의 무결성을 검사하고 오류를 검출하는 데 효과적이다. CV QKD는 신호의 위상 정보를 활용하므로, 레이저 소스와 전송 매체에서 발생하는 위상 잡음이 성능에 큰 영향을 미친다. 위상 잡음을 보정하지 않으면 신호의 정확한 복원이 어려워지고, 정보 전송 효율이 크게 감소하며 보안 분석에서 취약점이 발생할 수 있다.

이러한 후처리 과정이 제대로 이루어지지 않으면, CV QKD 시스템은 높은 오류율, 낮은 키 생성률, 그리고 보안 취약성과 같은 부정적인 결과를 초래할 수 있다. 따라서, 본 논문에서는 이러한 문제를 해결하기 위한 DSP 기술과 후처리 알고리즘의 방법을 보였다. 추후 본 시스템에서 추출한 데이터로 excess noise, secret key rate를 계산해볼 수 있을 것으로 보인다.

ACKNOWLEDGMENT

이 논문은 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원-대학ICT연구센터(ITRC)의 지원을 받아 수행된 연구임(RS-2021-II211810)

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

참 고 문 헌

[1] Karinou, Fotini, et al. "Toward the integration of CV quantum key distribution in deployed optical networks." IEEE Photonics Technology Letters 30.7 (2018): 650-653.

[2] Milovančev, Dinka, and Nemanja Vokić. "Monolithically Integrated Ultra-Low Noise Balanced Receiver for CV-QKD." 2024 47th MIPRO ICT and Electronics Convention (MIPRO). IEEE, 2024.

[3] Alsaui, Abdulmohsen, Yousef Alghofaili, and Deepa Venkitesh. "Machine learning and time-series decomposition for phase extraction and symbol classification in CV-QKD." Physica Scripta 99.7 (2024): 076008.

[4] Laudenbach, Fabian, et al. "Pilot-assisted intradyne reception for high-speed continuous-variable quantum key distribution with true local oscillator." Quantum 3 (2019): 193.