파일럿 톤 기반 LLO 연속변수 양자 키 분배 시스템 성능 분석

송주현, 허준*
고려대학교

sjuh1219@korea.ac.kr, *junheo@korea.ac.kr

Performance Analysis of Pilot-Tone-Assisted LLO CV-QKD Systems

Juhyun Song, Jun Heo*
Korea University

요 약

본 논문은 LLO 구조에서 발생하는 레이저 간 위상 드리프트 문제를 해결하기 위해, 주파수 영역에서 분리된 파일럿 톤을 이용한 QPSK 양자 키 분배 시스템을 제안한다. 강한 세기의 파일럿 톤을 양자 신호와 직교 편광으로 전송하고, 수신단에서 DSP 를 통해 이를 추출함으로써 위상 드리프트를 정밀하게 보상한다. 시뮬레이션 결과 실질적인 위상 드리프트 조건에서도 유효한 비밀 키 생성률을 달성함을 확인하였다.

Ⅰ. 서 론

양자 암호 키 분배(Quantum Key Distribution, QKD)는 양자역학적 특성에 기반한 정보 이론적 보안성을 제공함으로써, 양자컴퓨터의 발전으로 위협받는 현재의 암호 체제에 대한 대안 중 하나로 주목받고 있다. 특히 연속변수 방식(Continuous Variable QKD, CV-QKD)은 기존 광통신 인프라와의 호환성이 높아 비교적 저비용 구현이 가능하다는 장점으로 활발히 연구되고 있다[1]. 이 중 국부 발진기(Local Oscillator, LO)를 신호와 함께 전송하는 TLO (Transmitted LO) 구조는 실험적 구현이 용이하나, 전송된 LO 가 외부로 노출되어 도청자(Eve)에 의해 조작되거나 악용될 수 있다는 본질적인 보안 취약성을 내포하고 있다[2]. 이를 해결하기 위해서는 수신단에서 별도의 레이저를 사용하는 LLO (Local LO) 구조 도입이 필수적지만, 송수신기 레이저의 독립성으로 인해 발생하는 위상 드리프트가 실제 구현의 주요한 기술적 장벽이 된다.

이러한 한계를 극복하기 위해, 본 연구에서는 주파수 영역에서 분리된 파일럿 톤을 이용한 QPSK 기반 LLO CV-QKD 시스템을 제안하고, 시뮬레이션을 통해 이를 검증한다. 특히 직교 편광을 이용한 파일럿 톤 전송으로 신호 간 간섭을 최소화하며, 현실적인 레이저 선폭 조건에서도 안정적인 위상 보정을 통한 높은 비밀 키 생성률(Secret Key Rate, SKR) 달성이 가능함을 보인다.

Ⅱ. 본론

A. CV-QKD System Model

본 연구에서 제안하는 LLO CV-QKD 시스템은 송신단(Alice)에서의 QPSK 변조와 수신단(Bob)에서의 헤테로다인 검출을 기반으로 한다. QPSK 와 같은 이산 변조 방식은 가우시안 변조 대비 낮은 신호 대 잡음비(SNR) 환경에서 높은 재조정 효율(Reconciliation efficiency)을 달성할 수 있어 실용적 전송 거리를 확보하는 데 유리하다. 이때, 시스템의 핵심적인 위상 동기화는 주파수 및 편광 다중화된 파일럿 톤을 통해 이루어진다. 송신단에서 직교 편광으로 전송된 파일럿 톤은 수신단의 편광 분리기 (Polarization Beam Splitter, PBS)를 통해 효과적으로 분리되며, 디지털 신호 처리 (Digital Signal Processing, DSP)를 통해 실시간 위상 보정을 수행함으로써 시스템 보안성과 구현 편의성을 동시에 확보하였다.

B. Secret Key Rate Estimation

CV-QKD 의 보안 증명은 Alice 와 Bob 사이의 상관관계를 검증하여 Eve 가 획득 가능한 정보의 상한을 산출하는 과정이다[3]. 이러한 보안 분석은 Parameter estimation 절차를 통해 수행된다. 본 연구에서는 수신기의 전자적 잡음과 검출 효율을 Eve 가 통제할 수 없다고 간주하는 trusted-detector 모델을 가정하고, collective attacks 에 대한 Asymptotic SKR($K_{\mathrm{coll}}^{\mathrm{asymp}}$)을 다음과 같이 계산하였다[4].

$$K_{\mathrm{coll}}^{\mathrm{asymp}} = f_s[\beta\, I_{AB} - \chi_{BE}] \quad (1)$$

여기서 f_s는 sifting ratio, β는 reconciliation efficiency, I_{AB} 는 Alice 와 Bob 사이의 상호 정보량 (mutual information)이며, χ_{BE} 는 Bob 와 Eve 사이의 Holevo 정보량이다.

C. Simulation Design

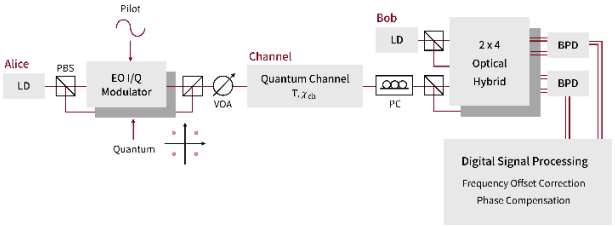


그림 1. 파일럿 톤 기반 LLO CV-QKD 모델

Alice 는 중심 파장 $\lambda = 1550$ nm, 선폭 400 kHz 인 레이저를 사용하여 250 Mbaud QPSK 데이터($V_A = 0.7$ SNU)를 생성한다. Bob 의 LO 는 20 kHz의 좁은 선폭을 갖는 이상적 광원으로 가정하였다. 이로 인해 발생하는 총 420 kHz 의 상대 선폭은 시스템의 열악한 위상 잡음 환경을 조성한다. 파일럿 톤은 1 GHz 오프셋되어 전송되며, 세기는 신호 대비 20 dB 높은 강도로 설정되어 정밀한 위상 추정을 가능하게 한다[5].

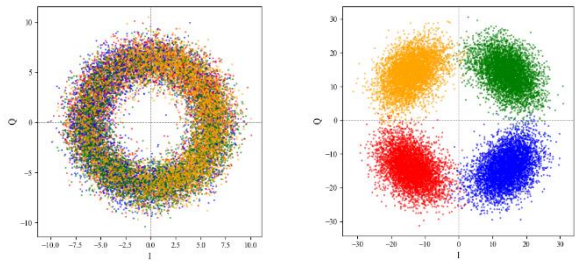
이때 양자 데이터와 파일럿 톤 간의 크로스토크를 최소화하기 위해 두 신호의 편광 방향을 직교하도록 설계하였다. 전송 과정에서 절대적인 편광 상태는 변화할 수 있으나, 두 신호 간의 상대적인 편광 차이는 유지되기 때문에 수신기에 도착한 신호를 PBS 와 편광 제어기(PC)를 이용하여 효과적으로 분리할 수 있다. 이를 통해 파일럿 톤을 삽입하면 대역폭과 동적 범위가 매우 큰 검출기를 요구하는 문제가 자연스럽게 해결된다.

광 전송 채널은 감쇠 계수 $\alpha = 0.2$ dB/km 인 표준 광섬유로 모델링하였으며, 전자적 잡음 $\nu_{el} = 0.1$ SNU 및 검출 효율 $\eta = 0.6$을 반영하였다.

D. Simulation Results

파일럿 톤의 위상 추적 결과, RMS phase tracking error 는 0.2270 rad 로 측정되어 QPSK 복조 허용 한계($\pi/4$) 내에서 안정적인 성능을 보였다. 이를 통해 제안된 파일럿 톤 기법이 높은 선폭을 갖는 실용적 구성에도 시스템 운용에 필요한 위상 일관성을 충분히 유지할 수 있음을 확인하였다.

위상 보정 효과를 가시적으로 확인하기 위해, 우선 $V_A = 100$ SNU 의 높은 변조 분산 조건에서 시스템을 평가하였다. 파일럿 톤 기반 위상 DSP 를 적용한 결과, 왜곡되었던 QPSK constellation 이 효과적으로 보정된 것을 확인할 수 있었다. 보정 후 BER 은 0.00267 로 감소하였으며, 이러한 복원이 누적된 위상 드리프트를 효과적으로 보상함을 입증하였다.



(a) 보정 전 (b) 보정 후

그림 2. $V_A = 100$ SNU 위상 보정 전후 Constellation

이후에는 실용적인 QKD 파라미터 환경에서 SKR 을 평가하기 위해 변조 분산을 $V_A = 0.7$ SNU 로 설정하여 분석을 수행하였다. 시뮬레이션 결과, 낮은 SNR 환경에서도, 25km 광섬유에 대해 3.48 Mb/s (0.0139 bits/symbol)의 유효한 SKR 을 달성하였다. 표 1 에서는 5km, 25km, 50km 에 대한 채널 투과율(Transmittance, T)과 SKR 산출 결과를 나타낸다. 그림 3 은 reconciliation efficiency 변화에 따른 채널 손실 대비 SKR 추이를 보여준다. attenuation 에 따라 SKR 은 감소하는 경향을 보이는데, 이는 광섬유 손실이 증가할수록 Alice 와 Bob 사이의 상관관계가 약해져서 I_{AB} 가 감소하기 때문으로 해석할 수 있다. 이러한 결과는 CV-QKD 시스템이 다양한 채널 거리 조건에서도 실질적으로 동작 가능함을 보여준다.

L (km)	T	SKR [bits/sym]
5	0.7943	0.0663
25	0.3162	0.0139
50	0.1000	0.0017

표 1. 전송거리에 따른 투과율 및 SKR

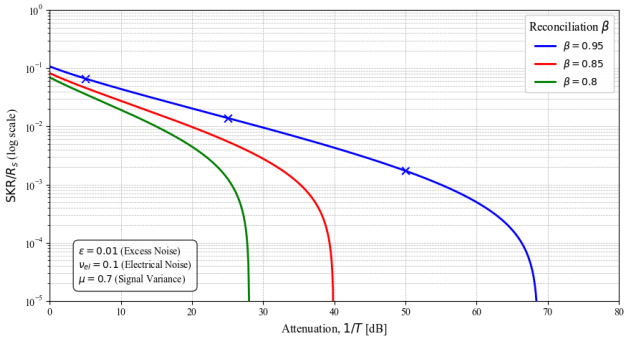


그림 3. 채널 손실 및 재조정 효율에 따른 SKR

Ⅲ. 결론

본 논문에서는 현실적인 광학 및 전자 잡음 모델이 통합된 시뮬레이션을 구축하여, 파일럿 톤 기반 DSP 가 적용된 LLO CV-QKD 시스템이 강한 위상 잡음 환경에서도 효과적으로 동작함을 입증하였다. 주파수 및 편광 다중화된 파일럿 톤을 이용한 위상 보정 기법은 총 레이저 선폭 420 kHz 의 조건에서도 0.2270 rad 의 정밀한 위상 추적 오차를 달성했으며, 이를 통해 25km 전송 거리에서 3.48 Mb/s의 SKR 을 달성하였다.

결론적으로, 제시된 위상 보정 기법은 하드웨어 기반의 phase-locking 방식보다 구현이 용이하면서도 LLO 구조의 보안상 이점을 극대화할 수 있는 실용적인 대안임을 확인하였다. 본 연구는 저비용·고속 양자 통신 시스템의 실험적 구현을 위한 이론적 토대를 제공한다는 점에서 그 의의가 있다.

ACKNOWLEDGMENT

본 연구는 한국연구재단의 양자정보과학 인적기반 조성사업의 연구결과로 수행되었음(RS-2023-NR068116).

참 고 문 헌

[1] T. C. Ralph, "Continuous variable quantum cryptography," *Phys. Rev. A*, vol. 61, no. 1, Art. no. 010303(R), 1999.

[2] F. Laudenbach *et al.*, "Pilot-Assisted Intradyne Reception for High-Speed Continuous-Variable Quantum Key Distribution With True Local Oscillator," *Quantum*, vol. 3, Art. no. 193, Oct. 2019.

[3] R. Wolf, Quantum Key Distribution: An Introduction with Exercises. Cham, Switzerland: Springer, 2021.

[4] A. Ruiz-Chamorro, A. Garcia-Callejo, and V. Fernandez, "Low-complexity continuous-variable quantum key distribution with true local oscillator using pilot-assisted frequency locking," Sci. Rep., vol. 14, Art. no. 10770, 2024.

[5] B. Schrenk and H. Hübel, "Pilot-assisted local oscillator synchronisation for CV-QKD," in Proc. Int. Conf. Quantum Cryptography (QCrypt), 2016, Art. no. 7.