WDM 채널 기반 One-way BB84 QKD 성능 계산

곽혜린, 허준*
고려대학교

lynkwak12, *junheo@korea.ac.kr

Performance Evaluation of One-Way BB84 Quantum Key Distribution over WDM Channels

Hye Lyn Kwak, Jun Heo*
Korea Univ.

요 약

양자컴퓨터의 발전으로 기존 RSA 암호체계의 보안성 한계가 제기되면서, 이론적으로 도청이 불가능한 양자키분배(QKD)가 주목받고 있다. 본 연구에서는 WDM(Wavelength Division Multiplexing) 채널에서 one-way BB84 프로토콜을 구현하여 QKD 신호와 일반 광통신 신호의 공존 실험을 수행하였다. 1550 nm 대역의 QKD 신호는 1310–1430 nm 대역의 4 개 OOK 신호와 함께 전송되었으며, Raman 산란 등의 비선형 노이즈를 줄이기 위해 25 GHz 대역폭의 필터를 적용하였다. 실험 결과, QKD 신호만 전송할 때의 QBER 은 17.28%, 일반 신호와 동시 전송 시에는 19.59%로 약 2%p 증가하였다. 본 연구는 WDM 기반 QKD 공존의 가능성과 한계를 제시하며, 향후 Cascade 오류정정 및 Privacy Amplification 을 통해 최종 보안 키 생성을 목표로 한다.

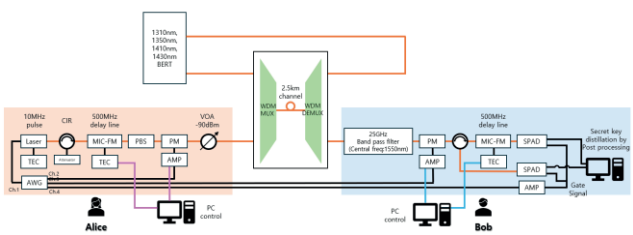
Ⅰ. 서론

양자 컴퓨터의 발전에 따라 현재 사용하는 RSA 암호화 체계가 무너질 수 있다는 우려와 함께 이론적으로 도청이 불가능한 개념의 양자 암호 통신이 개발되었다. 가장 대중적이며 상용화가 되어 있는 프로토콜인 BB84 프로토콜[1]을 구현함에 있어서는 단일 광자를 간섭계에 통과시킴으로써 양자 역학의 중첩 원리를 사용한다.

광자 단위의 신호를 측정하기 위해서 하나의 광통신 망 인프라를 구축하는 것은 자원 소모가 극심하므로, 현재 사용 중인 광통신 망에서 사용하는 WDM(Wavelength Division Multiplexing) 기술에 QKD 망을 같이 mux 하여 송신하는 아이디어가 제시된다. 본 논문에서는 WDM 채널에 one-way BB84 프로토콜을 송신하는 실험을 진행 뒤 raw QBER 을 계산해보고자 한다.

Ⅱ. 본론

실험의 setup 은 아래와 같다[2],[3].



10MHz pulse 기준 pulse 하나 당 광자가 1 개 존재한다고 가정하였을 때 송신해야 하는 power 는 -90dBm 이므로 attenuator 를 이용하여 Alice 의 신호를 감쇄한다. WDM MUX 에는 1310, 1350, 1410, 1430nm 대역의 일반 광통신 OOK 신호가 1550nm 대역의 QKD 신호와 함께 전송된다. WDM 과정에서 유선 광섬유를 다양한 파장대역의 신호가 지나가게 되며 비선형 노이즈인 Raman -scattering 등이 생기게 된다. 따라서 최대한 다른 대역의 노이즈를 제거하기 위해 WDM DEMUX 이후 25GHz 대역폭을 가진 band pass filter 를 이용한다. Filter 를 통과하면 QKD 신호의 wavelength pulse 만을 걸러내 깔끔한 신호 추출이 가능하다.

Alice 와 Bob 의 phase encoding, decoding 은 PRBS-7 PRNG 알고리즘으로 진행한다. DSP 는 matlab 을 이용한다. SPAD 의 detection out signal 은 10ns 의 pulse width 를 가진 TTL 신호이므로 250MHz sampling rate 로 acquisition 하여 25sample 을 1 symbol 로 상정하여 DSP 한다. Delay matching 을 위하여 greedy 방식으로 matching probability 가 가장 높은 부분을 채택하는 방법을 선택하였다. 이 때, DSP 완료 후 확인되는 QBER 을 비교한다. 비교 대상은 2.5km WDM 채널에 1550nm 대역 QKD 신호만 전송될 경우, 일반 광통신 신호 4 개와 QKD 신호를 같이 전송할 경우이다.

DSP 결과 도출되는 raw key QBER 은 아래와 같다.

```
A onsets: 236208,  B onsets: 1023
Best tau* = -4953 (score=0.0010, matches=229 / Avalid=235272)
Top-3 delays:
  #1: tau=-4953, score=0.0010, M=229, Avalid=235272
  #2: tau=4953, score=0.0010, M=229, Avalid=235272
  #3: tau=-4826, score=0.0010, M=229, Avalid=235296
C onsets: 236208,  D onsets: 1814
Best tau* = 4914 (score=0.0017, matches=396 / Avalid=235278)
Top-3 delays:
  #1: tau=4914, score=0.0017, M=396, Avalid=235278
  #2: tau=4787, score=0.0017, M=396, Avalid=235302
  #3: tau=4660, score=0.0017, M=396, Avalid=235326

--- Core-only Metrics (dead-time fully excluded) ---
Counts (core):  True_0=453, True_1=253, F2_0=210, F1_0=0, F2_1=376, F1_1=1, Total=8.534852e+02
Fdark=9.999000e-01, Fde=1.464854e+02
Eff_η  : ACC=0.8272, QBER=0.1728  (SPAD η=0.25)
>>
```

위 결과는 WDM 채널에 QKD 신호만 전송했을 경우이다. 채널 길이가 길어 17.28%의 raw key QBER 이 도출된다.

```
A onsets: 236208,  B onsets: 1007
Best tau* = 618 (score=0.0009, matches=221 / Avalid=236089)
Top-3 delays:
  #1: tau=618, score=0.0009, M=221, Avalid=236089
  #2: tau=491, score=0.0009, M=221, Avalid=236113
  #3: tau=364, score=0.0009, M=221, Avalid=236137
C onsets: 236208,  D onsets: 1662
Best tau* = -4915 (score=0.0015, matches=350 / Avalid=235278)
Top-3 delays:
  #1: tau=-4915, score=0.0015, M=350, Avalid=235278
  #2: tau=-4788, score=0.0015, M=350, Avalid=235302
  #3: tau=-4661, score=0.0015, M=350, Avalid=235326

--- Core-only Metrics (dead-time fully excluded) ---
Counts (core):  True_0=388, True_1=249, F2_0=210, F1_0=1, F2_1=407, F1_1=0, Total=7.922345e+02
Fdark=9.999000e-01, Fde=1.542346e+02
Eff_η  : ACC=0.8041, QBER=0.1959  (SPAD η=0.25)
>>
```

위 결과는 WDM 채널에 QKD 신호와 함께 4 개의 일반 광통신 신호를 같이 전송했을 경우 raw key QBER 이다. 2%p 의 QBER 이 증가한 19.59%인 점을 확인할 수 있다.

Ⅲ. 결론

본 논문에서는 one-way BB84 QKD 를 WDM 채널에 일반 광통신 신호와 같이 인가하였을 때 QKD 신호만 전송한 경우와의 QBER 을 비교한다. WDM 과정에서 비선형 노이즈인 Raman-scattering 등에 의한 영향이 생기나, QKD 신호만 통과할 수 있는 좁은 폭의 band pass filter 를 사용하여 그 영향을 최소화하고자 하였다. 이때, QBER 은 WDM 채널에 일반 광통신 채널을 인가하기 전보다 2%p 증가하는 결과를 보였다.

현재 QKD 신호만을 전송할 때도 QBER 이 매우 큰 상황이므로 추후 encoding, decoding 과정을 더 정교하게 진행하고 band pass filter 를 더 좁게 만들어 채널 통과 뒤에도 안정적인 QBER 을 도출해보고자 한다. 또, 최종적인 secret key 를 완성하기 위해 information reconciliation 기법인 cascade 알고리즘을 추가하여 QBER 을 낮추고, privacy amplification 을 추가하여 보안성을 높인 최종 key 를 추출 뒤 key rate 를 계산해보고자 한다.

ACKNOWLEDGMENT

이 논문은 정부(과학기술정보통신부)의 재원으로 한국연구재단 양자정보과학 인적기반 조성사업의 지원을 받아 (Grant No. 2022M3H3A1063074,50%), 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원(No. RS-2023-00242396,50%)을 받아 수행된 연구임

참 고 문 헌

[1] Bennett, Charles H., and Gilles Brassard. "Quantum cryptography: Public key distribution and coin tossing." *Theoretical computer science* 560 (2014): 7-11.

[2] Dejen, B., Vaquero-Stainer, A., Santana, T. S., Arabskyj, L., Dolan, P. R., & Chunnilall, C. J. (2024). A refined method for characterizing afterpulse probability in single-photon avalanche diodes. *Applied Physics Letters*, *125*(19).

[3] Mo, Xiao-Fan, et al. "Faraday-Michelson system for quantum cryptography." *Optics letters* 30.19 (2005): 2632-2634.