TCSPC 를 활용한 one-way BB84 양자 키 분배 간섭 확인 및 QBER 계산

곽혜린, 김범일, 허준*
고려대학교

lynkwak12, bik0118,*junheo@korea.ac.kr

Time-Correlated Single Photon Counting-Based Interference Characterization and Error Analysis in One-Way BB84 QKD

Hye Lyn Kwak, Jun Heo*
Korea Univ.

요 약

본 논문에서는 단일 광자보다 낮은 수준의 레이저를 간섭계에 통과시켜 양자 중첩 현상을 기반으로 하는 one-way BB84 프로토콜을 구현하였으며, 이를 바탕으로 양자 통신의 핵심 요소인 간섭 특성을 실험적으로 분석하였다. 특히 Time-Correlated Single Photon Counting(TCSPC)를 활용하여, 단일 광자 검출기(SPAD)의 출력 신호 도착 시간을 통계적으로 누적함으로써 간섭 패턴을 관찰하고, 양자 오류율(QBER)을 정량적으로 산출하였다.

.

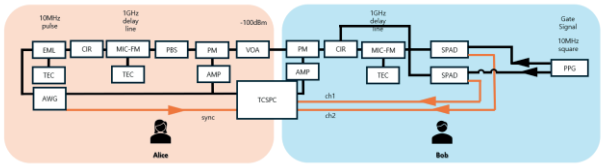
Ⅰ. 서 론

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.

TCSPC 를 활용하면 SPAD 의 detection out 출력부로부터 나오는 신호의 도착 시간을 토대로 count 를 integration 하여 쌓아 올릴 수 있고, detection 의 통계를 확인할 수 있다. 본 논문에서는 TCSPC 를 통해 단일 광자 수준의 laser 의 양자 역학적 중첩을 확인해보고자 한다.

Ⅱ. 본론

실험의 setup 은 아래와 같다[2],[3].

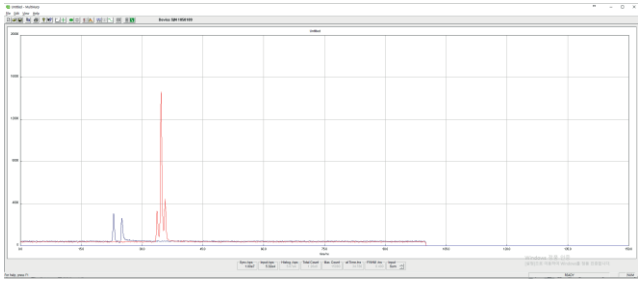


대부분의 DV-QKD 는 decoy method 를 채용하여 사용하고 있다. 10MHz repetition rate 를 가진 laser pulse 하나 당 1 개의 광자가 있다고 가정한다면, -90dBm 으로 attenuation 하여 전송하면 되지만 decoy method 를 채용하면 0.1 mean photon number 와 같이 single photon number 보다 작은 power 로 attenuation 하여야 키의 보안성을 확보할 수 있다. 따라서 Alice 는 phase modulation 된 신호를 -100dBm 으로 송신하게 된다.

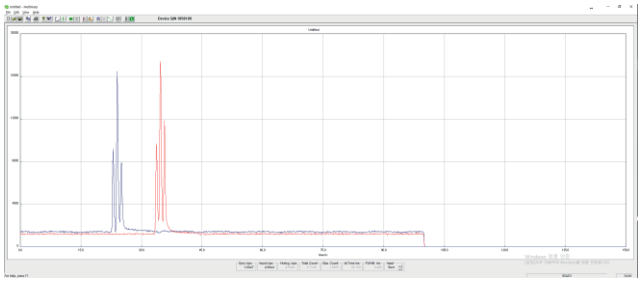
SPAD 는 decoding 이 완료된 신호를 gated mode 로 관측한다. SPAD 는 소자의 특성 상 한 번 detection 이 되면 ns~μs 의 dead time 이 생성되고, 이 동안은 gate 신호가 인가되어도 detection 이 진행되지 않는다. SPAD 는 detection 이 되자마자 detection out 으로 TTL 신호를 출력한다.

TCSPC 는 sync channel 대비 다른 channel 에서 들어오는 신호가 얼마나 늦는지를 판별하여 주는 장치이다. 따라서 AWG 에서 10MHz 의 sync 를 인가하여 주고, 두 개의 SPAD 는 TCSPC 의 두 채널과 연결된다.

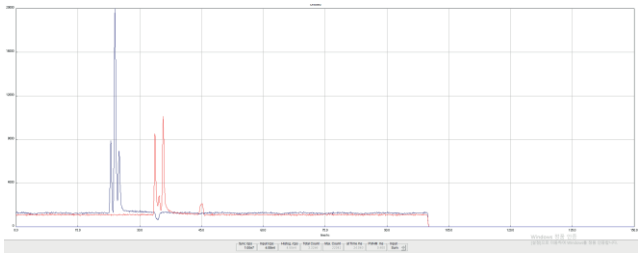
Alice 와 Bob 에 encoding, decoding 을 전부 진행하지 않을 경우 TCSPC 에서 관측되는 모습이다. TCSPC 에서 관측하는 모습은 330 만개의 count 를 합쳐서 integration 한 그래프이므로 detection 의 통계를 확인할 수 있다.



Alic 에 0, Bob 에 0 의 phase encoding, decoding 을 진행한 뒤의 모습이다. 파란 색의 Ch1, 빨간 색의 Ch2 가 각각 상쇄 간섭과 보강 간섭으로 나타나는 것을 확인할 수 있다. SPAD 는 신호가 들어오지 않아도 신호가 들어왔다고 인식하는 dark count 가 있는데, 이 또한 오류로 판단된다. Dark count 에 의한 QBER 은 3.21%로 계산할 수 있다.



Alice 에 $\pi/2$, Bob 에 0 의 phase encoding, decoding 을 진행한 뒤의 모습이다. BB84 의 특성 상 basis 가 맞지 않아 확률적으로 Ch1 과 Ch2 모두에서 detection 이 되고 있는 모습이며, 이 경우는 양자역학의 중첩 원리가 보여지는 상황이고 key 로써 활용할 수 없다. 따라서 QBER 도 계산하지 않는다.



Alice 에 π, Bob 에 0 의 phase encoding, decoding 을 진행한 뒤의 모습이다. 0, 0 encoding decoding 과 비교하면 채널의 간섭이 뒤바뀐 모습을 확인할 수 있고, 이 경우는 둘의 basis 는 같으나 bit 가 flip 된 상태라 할 수 있다.

다만 Alice 에 π modulation 을 진행했을 때 완벽한 상쇄 간섭 pattern 으로 나타나지 않아 이 부분은 key error 가 된다. 이는 QBER(Quantum Bit Error Rate)라 할 수 있고 key rate 감소에 영향을 줄 수 있다. TCSPC 의 측정 count 를 참고하여 QBER 을 계산하면 8.89%로 확인할 수 있다. 추후 연구에서 현재의 setup 을 WDM 네트워크에 연결할 것인데, WDM 네트워크를 통과하는 동안 Raman scattering, FWM(Four wave mixing), 기타 crosstalk 등의 영향이 심하므로 최대한 modulation 으로부터 만들어지는 key error 는 줄여야 하므로 modulation error 를 줄이는 연구를 진행해보고자 한다.

Ⅲ. 결론

본 논문에서는 one-way BB84 QKD 의 setup 을 완성하고, decoy method 도 활용하기 위하여 0.1 mean photon power 로 attenuation 시킨 뒤 간섭 패턴을 확인하고 QBER 을 계산하는 과정을 거쳤다. SPAD 의 dark count 에 의한 오류는 소자 특성이므로 줄일 수 없으나, modulation 에 의한 오류를 줄이고자 연구를 진행해야 한다. 추후 WDM 네트워크에 QKD 신호를 추가한 뒤의 error 패턴을 분석하고 QBER 을 낮춰 key rate 를 높이는 방법을 확인해보고자 한다.

ACKNOWLEDGMENT

이 논문은 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원-대학 ICT 연구센터(ITRC)의 지원(RS-2021-II211810, 50%)과 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.