양방향 양자키분배 시스템에서 전송거리에 따른 오류율 측정

Measurement of distance-dependent quantum bit error rate in two-way quantum key distribution systems

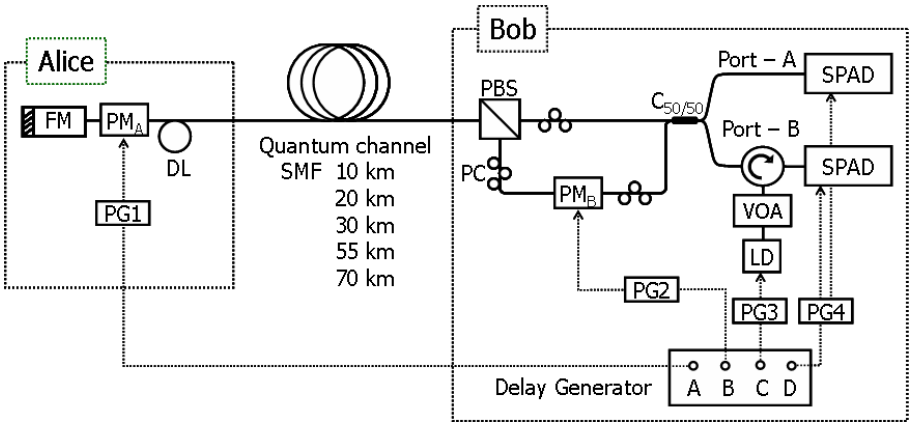
이승훈, 정규현, 김승환, 이민희, 김경헌
인하대학교 물리학과
lsh@inhaian.net

본 논문에서는 장거리 양자암호 전송에 있어서 광섬유 전송 거리에 따른 오류율을 측정한 연구 결과를 소개한다. 특히 외부 환경에 안정된 양방향 양자 암호 전송 기술의 하나인 plug-and-play 방식의 구도에서 전송 거리를 극대화하는 노력에 있어서 가장 문제시되는 Raleigh-backscattering의 효과에 의한 양자비트 전송에서의 오류를 측정하였다. 아울러 이러한 오류를 최소화하면서 70 km 단일모드 광섬유 전송을 구현한 양자통신 결과를 소개하고자 한다.

근래에 들어와 활발한 연구와 실용화가 추진 중인 양자통신 기술에 있어서 양자 암호키 전송 속도 및 전송 거리의 증가와 더불어 양자 중계 및 네트워크 기술이 주요 기술적 이슈가 되고 있다. 현재 양자암호 기반 보안통신 시스템은 상용제품이 나오는 수준이기도 하나, 아직 낮은 전송 속도와 제한적인 전송 거리 수준에 머물고 있다.(1) 양자암호 통신은 공공의 통신채널을 통해 암호문을 전송하고 단일광자의 양자상태를 이용하여 암호문을 해독할 수 있는 비밀키를 생성하여 공유함으로써 물리적으로 보안이 보장되는 기술이다. 이러한 양자암호의 핵심이 되는 비밀키를 광학계를 통해 생성하고 송신자와 수신자가 나누어 가짐으로써 이 암호키를 전송하는 과정을 양자키분배 (Quantum Key Distribution; QKD)라 한다. 1993년에 처음으로 P.D. Townsend 등에 의해 10 km 길이의 광섬유를 이용하여 전송된 광자의 간섭 실험이 있은 이후로 전송 거리와 비밀키의 생성률을 증가시키기 위해 새로운 프로토콜의 개발, 광학계의 개선, 저 잡음 및 고속의 단일광자 검출기 개발 등의 노력이 계속되고 있다.(2)

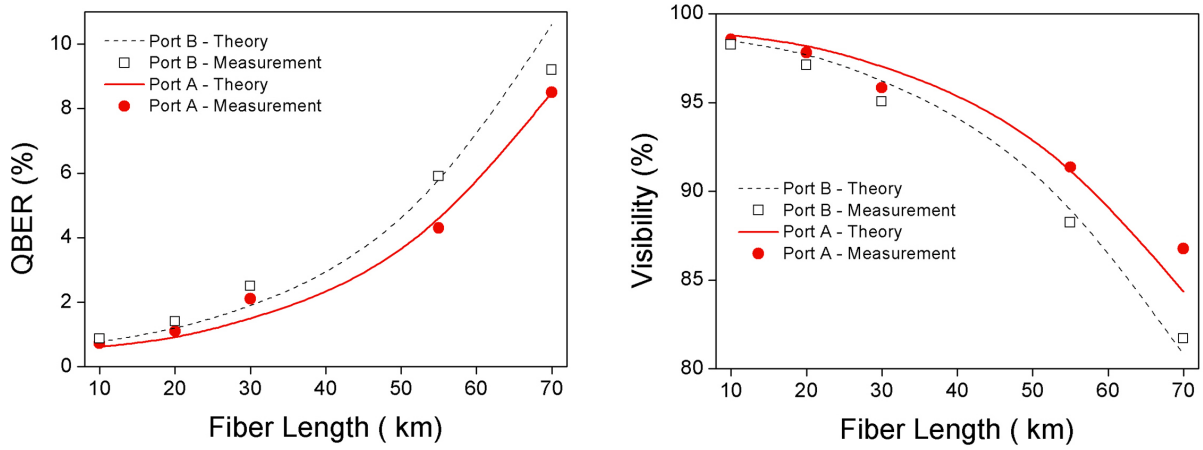
외부 환경의 변화에 대해 안정도가 높은 QKD 방식인 plug-and-play 방식은 양방향형의 양자 암호 전송 기술로서 상용화 시스템에도 활용이 되고 있는 방식이나 레일리 산란(Rayleigh scattering)에 의한 전송 거리 및 속도에 제한을 받고 있다[그림1]. 이 방식에서는 비대칭형 마흐젠더 간섭계가 Bob(수신자)에만 설치되어있고, Alice(송신자)에는 위상변조기와 패러데이 거울만이 있다. 먼저 Bob에서 Alice로 강한 레이저 펄스를 전송한다. Alice에 도착한 광펄스는 광커플러로 분리하여 일부는 Alice의 위상변조기를 구동시키는 동기신호로 사용하고 남은 광펄스는 패러데이 거울에서 반사되어 다시 Bob에게로 전송된다. 반사된 광펄스를 단일 광자수준으로 감쇄시키고 위상정보를 코딩하여 비밀키를 생성하게 된다. 패러데이 거울을 사용하여 편광을 90°회전시킴으로써 간섭하는 두 광 펄스들은 정확히 동일한 광 경로를 진행하게 되고, 광섬유 전송 선로에서 발생할 수 있는 편광 및 위상의 변화가 자동으로 상쇄되어 안정적인 간섭결과를 얻을 수 있다.(3) 그러나 광 펄스가 Alice 쪽으로 진행할 때 광섬유에서 레일리 산란이 발생하여 QBER(Quantum bit error rate)을 증가시키는 심각한 문제를 발생시킨다. 이러한 문제점은 연속 펄스열(Train Pulse)를 사용하고 저장 광섬유(Storage line)를 Alice에 추가하여 해결 할 수 있지만, 펄스열이 왕복한 이후에 다시 광펄스들을 보내야 하므로 장거리 및 고속의 양자키분배가 어렵다.

본 논문에서는 기존에 제안된 펄스열을 사용하는 방식 대신에 Bob에서 출발하는 초기 광펄스의 세기를 약하게 한 연속 펄스를 사용하여 레일리 산란에 의한 오류를 최소화 하여 장거리 전송 및 고속의 비밀키 생성이 가능하도록 하였다. 실험 장치는 [그림 1]과 같다. 사용한 레이저 다이오드의 반복률은 1 MHz, 단일광자 검출기의 효율은 15% 이고 Dark count 확률은 2.4 x 10^{-5}/(2-ns pulse) 이다.



[그림 1] 양방향 양자암호 키 분배 시스템

전송 광섬유의 길이를 변화시키며 양자 간섭 가시도와 QBER을 측정하고 이론값과 비교하여 [그림 2]에 나타 내었다. 이론에 의하면 QBER 이 11% 이하일 때 양자키분배의 안정성이 보장[4] 되는데 결과에 의하면 이번에 구성한 시스템은 70 km 까지 양자키 분배가 가능함을 알 수 있다.



[그림 2] 전송 거리에 따른 QBER 과 양자 가시도

[그림 2] 의 그래프를 보면 port B 의 QBER이 더 큼을 볼 수 있는데, 이는 port B 의 circulator 의 손실 때문이다. 따라서 간섭계를 구성하는 광 부품들의 개선을 통해 전송거리를 더욱 늘릴 수 있을 것으로 기대한다.

1. www.idquantiq.com
2. Seoung hun Lee, *et al*, "Low-Noise Single-Photon Detector for the 1.5-um wavelength Region", JKPS 50, 1-5 (2007).
3. D. Stucki, *et al*, "Quantum key Distribution over 67 km with a Plug & play system", New J. phys. 4, 41.1-41.8 (2002)
4. N. Lütkenhaus, "Estimates for practical quantum cryptography", Phys. Rev. A 59, 3301 (1999)