

## 양자 키 분배를 위한 양방향 시스템에서의 광자 간섭

### Photon interference in two-way system for quantum key distribution

이승훈, 정규현, 김승환, 김경현

인하대학교 물리학과

lsh@inhaian.net

최근 10여 년 동안 많은 연구자들에 의해 광섬유기반의 양자 키 분배 실험이 실현되었으며, 양자 키의 생성률을 증가시키고 전송거리의 한계를 극복하기 위한 노력이 계속 되고 있다.<sup>(1)</sup> 이러한 장거리 양자 키 분배는 광자의 위상을 무작위적으로 선택하여 키를 생성하는 위상코딩 BB84 프로토콜을 사용하는 것이 일반적이다. 송신부(Alice)와 수신부(Bob)를 위상변조가 가능한 비대칭 마흐젠더 간섭계로 구성하면 간섭의 결과를 통해 "0"과 "1"의 디지털 신호로 이루어진 암호 키를 얻을 수 있다.

양자 키 분배 시스템에 있어서 핵심적인 요소들은 단일광자광원, 정보 코딩을 위한 광학계 그리고 단일광자 검출기이다. 이중 광학계는 기존의 통신용으로 상당히 잘 개발되어있고 확정적인 단일광자 광원의 이용은 연구 단계이므로 현재 양자 키 분배의 효율을 증가시키는 가장 빠른 방법은 단일광자 검출기의 개선이라 할 수 있다. 본 연구에서는 InGaAs/InP APD를 gated Giger-mode로 동작하여 고효율, 저잡음을 갖는 1.5 um 파장영역의 단일광자 검출기를 제작하여<sup>(2)</sup> 양자 키 분배 시스템에 적용하였다. 실험구도는 그림1에 나타난 바와 같이 양방향 시스템으로 Plug and Play type<sup>(3)</sup>으로 알려져 있다. 패러데이 거울을 사용하여 광섬유에서의 복굴절이 자동적으로 보상되며, 광경로가 완벽히 동일하여 외부환경에 의한 편광 및 위상의 변화가 주는 가시도의 저하 현상을 줄일 수 있어 실험의 구성이 비교적 쉽다.

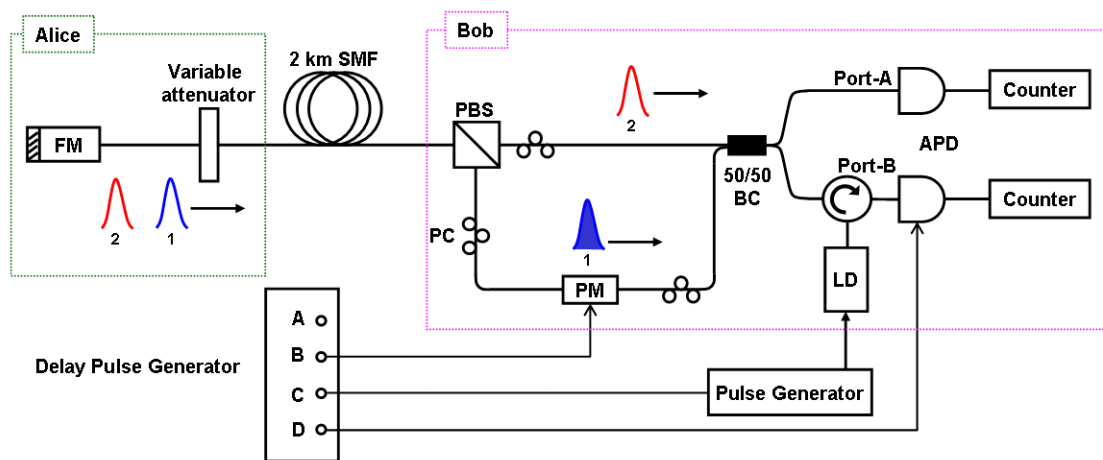


그림 1 양방향 양자암호 키 분배 시스템

DFB 레이저 다이오드를 이득 스위칭하여 발진시킨 파장 1.55  $\mu\text{m}$ , 반복률 141 kHz, 폭 40 ps 의 광 펄스를 circulator를 통하여 50/50 커플러에 입력시켰다. 커플러를 지난 광 펄스는 길이가 다른 경로를 지나 70 ps 만큼의 시간 차이를 갖고 편광빔분기기(PBS)에 도착한다. 이때 편광조절기(PC)를 이용하여 PBS에 입력되는 분할된 두 광 펄스의 편광이 서로 수직하게 하고 두 광 펄스 모두 Alice에게로 진행 할 수 있도록 하였다. 가변광감쇄기를 통과하는 광 펄스는 펄스당 평균 광자수를 0.1 photon 이 되도록 하였으며, 패러데이 거울에서 반사된 두 펄스는 입력대비 출력 광의 편광이 90도 회전하므로 Bob의 PBS에 도달하여서는 온 경로와 다른 경로를 택하게 된다. 따라서 두 광펄스 1, 2는 동일한 광경로를 진행하게 되며 50/50 커플러에서 간섭을 일으킨다. 이때 긴 경로에 PZT type의 위상변조기(PM)에서 위상을 임의로 변조시키면 위상 차에 따라 광자는 port-A 와 port-B 둘 중 하나의 포트로만 출력되게 할 수 있다. 그림2는 위상변조기에 인가하는 전압을 바꾸어 위상변조의 크기를 변화시킴에 따라 단일광자검출기에 나타나는 카운트 수를 측정된 결과이며, 그림 3은 측정에 사용된 단일광자 검출기의 효율을 측정된 그래프이다.

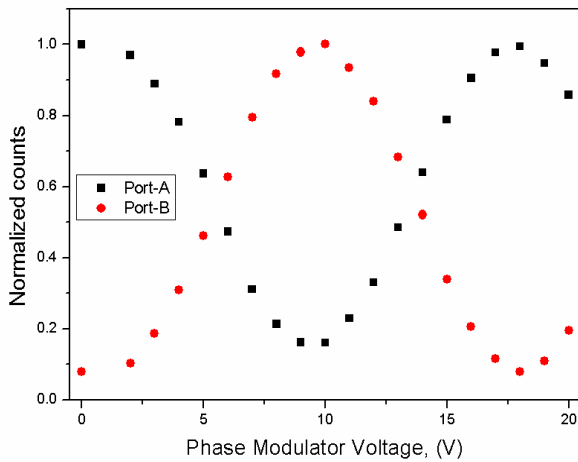


그림 2 위상변조기의 인가전압에 따른 광자 카운팅

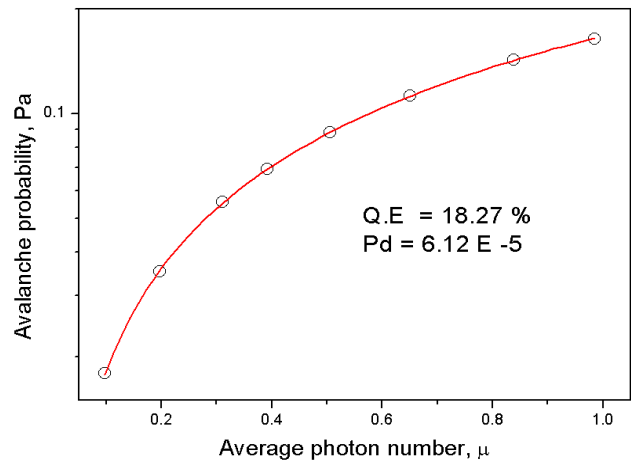


그림 3 단일광자 검출기의 효율 측정

Port-A 와 Port-B에서 광자 카운트에 의한 측정값으로 가시도(Visibility)를 계산하면 각각 0.72, 0.84 이며 QBER 은 13.8 %, 7.3 % 이다. 이러한 결과는 광섬유 및 커플러에서의 반사로 인해 생기는 잡음 때문이며, 이 잡음을 검출기의 Dark counts 수준으로 낮추면 가시도는 99 % 이상, QBER은 1% 이하의 값을 얻을 수 있을 것으로 기대한다.

본 연구에서는 자체 제작한 1.5  $\mu\text{m}$  파장대역 단일광자 검출기를 양방향 양자 키 분배 시스템에 적용하여 위상변조에 의한 광자간섭을 광자계수 방법으로 측정하였다. 본 연구는 학술진흥재단의 2단계 BK21사업-양자정보 및 디스플레이 광학 연구사업팀의 지원으로 수행되었음[핵06A2810].

참고문헌

1. N. Gisin et al, "Quantum Cryptography", Rev. Mod. Phys. 74, 145-195 (2002).
2. Seung hun Lee et al, "Low-Noise Single-Photon Detector for the 1.5- $\mu\text{m}$  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)