# 양자 암호화를 위한 양자 키 분배 시스템의 구성 설계
# Design of Quantum Key Distribution System for Quantum Cryptography

김인수*, 김요희*, V. E. Strigalev**
*한국전기연구원 정보-광응용연구그룹, **St. Petersburg State Univ. of Telecomm.
iskim@keri.re.kr

## 1. 서 론

오늘날에도 RSA암호문은 현대 암호에 대부분 적용될 정도로 안전하다고 생각되어왔다. 또한 PGP(Pretty Good Privacy)라는 가장 대중적인 암호화 소프트웨어도 RSA 원리를 기반으로 하고 있다. 그러나 RSA암호화체계는 주요한 결점이 있다. 인수분해하는 것이 "어렵다"라고 하지만, 결코 증명되지 않았고, 또한 인수분해를 수행하는 아주 빠른 알고리즘의 존재가 전혀 불가능하지는 않기 때문이다. 따라서 현존하는 암호화 체계보다 더 확실한 안전을 보장해주는 새로운 암호화 체계와 암호화키의 분배시스템의 필요성이 대두되고 있다.

## 2. 시스템의 구성설계 및 동작

양자 키 분배(QKD: Quantum Key Distribution)의 광학계의 구성도를 그림1에 나타내었다. 패러데이 거울(FM1, FM2, FM3)를 사용하여 간섭계에서 어떤 복굴절도 보상되며, 광로가 같아 외부환경변화가 시스템에 영향을 주지않아, 광학적인 정렬이 필요없는 구조로 구성하였다. 간단하게 동작을 기술하면, Bob측에서 짧은 레이저 펄스를 보내는데, 이것은 F(fast)와 S(slow)의 2개의 펄스로 나누어진다. F펄스는 Alice측으로 바로 갔다가 되돌아오는 반면, S펄스는 Bob측에 있는 2개의 FM으로 형성되는 지연라인인 FM1-FM2를 먼저 경유한 후에 Alice측에 갔다가 다시 Bob측으로 되돌아온다. Alice측에서는 단지S 펄스에 대해서만 위상변조기A를 사용하여 비트값을 encode하고, Bob측에서는 위상변조기B를 사용하여, FS 펄스에 대해서만 위상변조시킨다. 여기서 FS 펄스는 Bob측의 지연라인인 FM1-FM2를 통과하지 않은 F 펄스가 Alice측에 갔다가 Bob에 되돌아와서는 지연라인인 FM1-FM2을 통과한 펄스이고, 이것과는 경로가 반대인 SF는 Bob측에서 먼저 지연라인인 FM1-FM2을 통과한 후에 Alice측에 갔다가 Bob측에 되돌아와서는 지연라인인 FM1-FM2을 통과하지 않고 바로 도달한 펄스를 나타낸다. 또한 F 펄스가 Alice측의 수광소자 PD A에 도착할 때, Alice는 Alice측의 감쇄기로 단일 광자 레벨까지 얼마나 감쇄시켜야 할 지를 알기 위하여, 펄스의 에너지를 측정하고, 또 언제 펄스를 위상변조시킬지를 알기 위해 시간을 측정한다. 시스템의 timing은 클럭 발생장치에 의해 제공하고, 이것은 laser 펄스 발생기를 트리거시키고, function 발생기를 통하여 위상변조기에 공급한다. 또한 B92 프로토콜을 적용하여, Alice와 Bob의 비트값 "0"과 "1"에 대응하여, 0과 $\pi$의 위상천이를 통하여 변조시킨다. 만약 Alice와 Bob의 위상천이의 차가 0이면, SF와 FS 펄스들 사이에 constructive 간섭으로 PD B에 감지가 되고, 그들의 위상천이의 차가 $\pi$이면, SF와 FS 펄스들 사이에 destructive 간섭으로 아무것도 감지되지 않는다. 여기서 아무것도 감지되지 않을 때의 bit는 버린다. 그후에 Bob이 Alice에게 간섭이 constructive였는지 또는 destructive였는지를 알리면, 양쪽 다 그들이 같은 위상변조를 사용했는지를 알 수 있다. 그 다음은 같은 것만을 선택하여, 키로 같이 사용하면 된다. 그리고 이러한 광학적 구조설계를 바탕으로 하여 기본적인 실험을 할 수 있도록 설계한 큰 신호 모드에서 동작하는 QKD 시스템의 Alice측 시스템 블록도를 그림 2에, Bob측 시스템 블록도를 그림 3에, 그리고 이들의 시스템의 주요부분에서 각 신호들의 시간에 따른 신호파형을 그림 4에 표시하였다. 그림 3에서, Bob의 클럭발생기는 free 모드로 작동하고, Bob의 PRS(pseudo random sequence)는 계속적으로 동작한다. 그러나 광원 LD B가 정지하면 Bob측의 컴퓨터에 공급하는 신호인 인터럽트 펄스신호도 정지한다. 만약 PRS B의 레벨이 high(논리 1)이면, Delay

Modulator Bob은 Bob의 변조기에 공급하기위한 양의 펄스를 준비한다(논리1). 변조기의 펄스는 FF,FS,SF,SS 펄스신호가 Alice로부터 Bob에 되돌아오기전에 시작해서, 그들 펄스신호들이 도착한 후에는 끝내야 한다. Former strobe B는 Bob의 비교기(Comparator B)를 위해 gate를 만들기 위해 사용된다. 이 gate는 FS와 SF 펄스신호가 도착할 때는 open 해야한다. 만약 간섭이 constructive이면, 비교기의 레벨은 high이고 Pulse former PD B to PC는 Bob의 컴퓨터를 위해 긴 펄스를 만들어준다. Key-Start Stop이 동작할 때(on 일때), LD B는 빛을 발생시키고, Bob측의 컴퓨터( PC B )는 PRS B와 Bob의 수광소자로부터 데이터를 획득하기 시작한다. 획득될 수 있는 비트 수는 미리 정해놓는다. 컴퓨터가 이 숫자만큼 데이터를 획득하면, 일련의 과정이 중지된다. 그림 2에서, Alice는 PD A를 통해서 강한 F 펄스을 받는다. 비교기는 Alice의 PRS와 Delay Modulator Alice와 Interrupt pulse for PC A 들을 트리거하기 위해 짧은 펄스를 만든다. Alice측의 컴퓨터 ( PC A)는 단지 Alice의 PRS만 획득하고, 획득하는 수는 Bob의 시스템처럼 미리 정해둔다. Alice의 컴퓨터가 이 숫자만큼 데이터를 획득하면, 일련의 과정을 중지시킨다. Alice의 변조기를 동작시키는 시간을 갖기 위해 부가적인 광섬유 지연 선로가 필요하다. 이 Alice의 변조기는 F 펄스가 도착하는 시간과 S 펄스가 도착하는 시간사이에 동작시켜야 한다.

## 3. 결 론

본 연구에서는 QKD의 광학적 구조를 FM을 사용한 광섬유 비대칭형 Michelson간섭계 구조로 설계하여 어떠한 복굴절도 보상되며, 외부환경변화에 따른 광학적인 정렬이 필요없는 구조로 구성하였으며, 또 큰 신호 모드로 동작되는 전기, 광학적 시스템을 설계하였다.

본 연구는 과학기술부의 국제공동연구개발사업의 지원으로 수행되었음[M1-0105-00-0050].

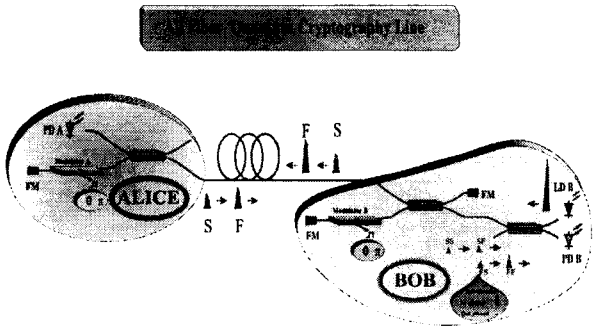


그림 1. QKD의 광학적 구성 설계도

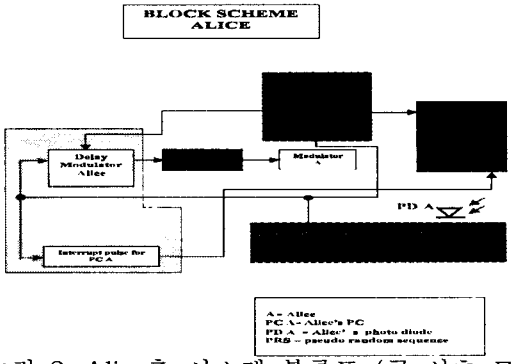


그림 2. Alice측 시스템 블록도 (큰 신호 모드)

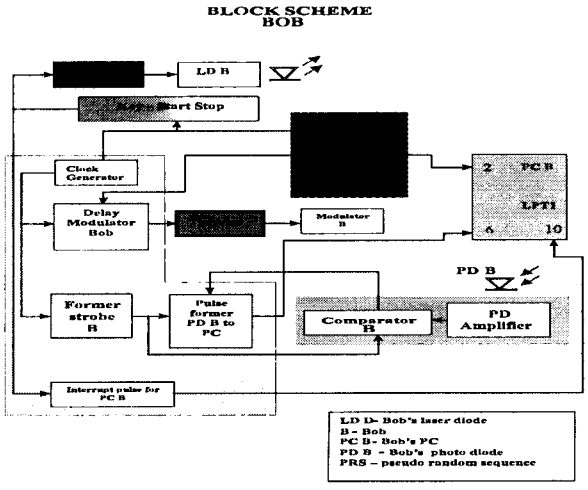


그림 3. Bob측 시스템 블록도 (큰 신호 모드)

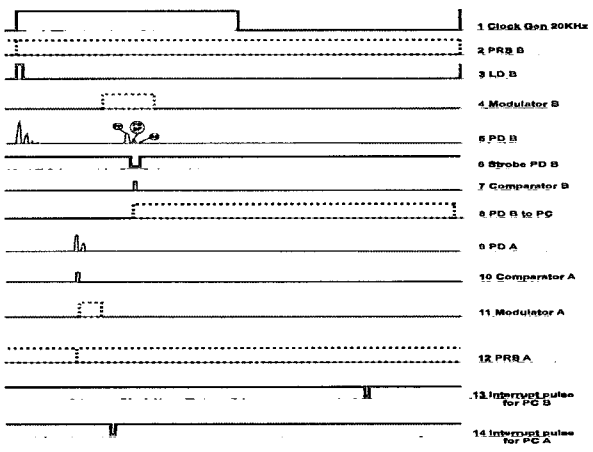


그림 4. 각종 신호들의 Time chart