위상안정화 광섬유를 이용한
단일방향 양자암호시스템에 관한 연구

연세대학교 대학원

전기전자공학과

박 준 범

위상안정화 광섬유를 이용한 단일방향 양자암호시스템에 관한 연구

지도교수 최 우 영 · 신 현 준

이 논문을 석사 학위논문으로 제출함

2006년 12월 일

연세대학교 대학원

전기전자공학과

박 준 범

박준범의 석사 학위논문을 인준함

심사위원 _____ 인

심사위원 _____ 인

심사위원 _____ 인

연세대학교 대학원

1999년 12월 일

감사의 글

오늘의 이 논문을 쓰기까지 도움을 주신 많은 분들이 있었기에 부족하나마 학위 과정을 마무리할 수 있었습니다. 모두 일일이 찾아 뵙고 감사의 말씀을 드리지 못함을 죄송스럽게 생각합니다.

먼저 학교 연구실에서 함께 한 시간은 부족했지만 연구 진행에 있어서 언제나 좋은 말씀과 격려로 저를 여기까지 이끌어 주신 최우영 지도교수님께 진심으로 감사드립니다. 또한 바쁘신 와중에도 논문 심사와 조언을 해주신 한상국 교수님께도 감사의 말씀을 드립니다.

이 연구를 진행함에 있어서 많은 도움을 주신 광주과학기술원의 한원택 교수님과 주성민 연구원님께도 감사의 말씀을 드립니다.

저의 석사생활 거의 대부분을 보낸 한국과학기술연구원의 많은 분들에게도 감사의 말씀을 드립니다. 저에게 한국과학기술연구원에서의 연구생활은 연구 뿐만이 아니라 인생에 있어서 많은 것을 얻은 공간입니다. 바쁘신 와중에도 항상 지켜봐 주시고 논문 및 연구내용에 대한 조언과 지원을 아끼지 않으셨던 문성욱 박사님께 진심으로 감사의 말씀을 드립니다. 연구실 생활에 있어서 박사님께서 보여주신 하나하나의 관심과 배려는 저와 학생들에게 큰 힘이 되었습니다. 감사합니다. 미국에서 박사후 과정에 바쁘신 와중에도 저의 논문과 연구지도에 아낌이 없으셨던 신현준 지도박사님께도 감사의 말씀을 드립니다.

Optical MEMS 연구실 연구원 가족 여러분들에게도 감사의 말씀드립니다. 석사 생활동안 느낀 점 중에 한가지가 혼자할 수 있는 일은 없다입니다. 여러분과 함께 연구를 하였기에 지금의 제가 있는 것 같습니다. 지금은 졸업을 하여 회사를 꾸려나가시느라 여념이 없으신 용희형과 근태형에게도 감사의 말씀을 드립니다. 그리고 연구실 맏형으로서 언제나 학생들 고민부터 시작해서 연구실의 대소사를 자신의 일처럼 신경을 써주신 승훈 형에게도 감사의 말씀을 드립니다. 그리고 한국말을 배우라고 해도 별 진전이 없던 Chi Anh, 그리고 연구실 동갑내기로 서로 힘이 되어 주었던 철우, 형원, 진혁이, 그리고 오토전자의 이성현 팀장님, 광호, 병규형, 유재욱씨, 호원, 경운, 민영, 무현, 병철, 호원, 영근, SL의 황차장님, 장식씨에게도 감사의 말씀을 드립니다. 지금은 연구실에 없지만 대석형, 영수형, 일진형, 홍일점인 미숙에게도 감사 드립니다.

특히나 저와 2년5개월을 함께한 양자암호팀의 철우와 경운이, 처음에는 많이 힘들었지만 서로의 일을 자기 일처럼 함께하였기에 지금의 우리가 있었던 것 같

습니다. 철우는 회사에 가서도 잘 하리라 믿고, 경운이도 앞으로 남은 1년동안 전에도 그래왔듯 앞으로도 잘 하리라 믿습니다.

마지막으로 제가 대학원까지 공부할 수 있도록 뒷바라지해 주신 아버지, 어머니와 동생 준모한테도 진심으로 감사의 말씀 드립니다. 또한 공부하는 사위를 따뜻하게 지켜봐주신 장인어른, 장모님께도 감사의 말씀 드립니다. 특히나 석사를 마치기까지 여러 가지로 힘이 들었을 텐데 아무 내색 없이 힘이 되어준 사랑스런 아내에게 사랑한다는 말과 함께 고맙다는 말을 전하고 싶습니다.

2006년 12월

차 례

그림 차례

표 차례

국 문 요 약

위상안정화 광섬유를 이용한
단일방향 양자암호시스템에 관한 연구

본 논문에서는 단일방향 구조의 양자암호 시스템 안정성 향상을 위해서 위상안정화 광섬유를 적용한 단일방향 양자암호 시스템을 제안한다. 양자암호시스템의 기본 구조인 단순 간섭계를 구현하여 위상안정화 광섬유의 안정성의 특성을 파악하였으며 비대칭 Mach-Zehnder 간섭계 구간에 위상안정화 광섬유를 적용하여 정밀한 온도 제어 시스템 없이 단순 단열을 통해 단일방향 양자암호 시스템을 구현하였다. 또한 단일광자검출기를 구현하여 이의 특성을 파악하였다. 제안된 시스템의 위상 변이는 평균 0.00153 π/sec, 최대 0.0024 π/sec가 측정 되었으며 이는 0.00027 π/sec의 위상 변이를 보인 다른 연구진의 결과와 비교하여 불안정한 결과이지만 여타 연구진의 단일방향 시스템의 위상 변이보다는 안정한 결과이다. 간섭계 구성에 전체적으로 위상안정화 광섬유를 사용하지 않았다는 점을 고려할 때, 전체적인 위상안정화 광섬유를 적용하게 되면 안정성이 더욱 향상 될 것으로 보인다. 또한 정교한 광학계 구성과 단열을 통해 plug & play 수준의 안정성을 단일방향 시스템에서 보일 수 있을 것으로 기대 되며 나아가 상용화 수준의 시스템 제작이 가능할 것으로 예상된다. 구현된 시스템의 간섭계 정확성을 측정하기 위해서 visibility를 측정하였으며 전송거리 25km에서 91%의 visibility를 나타내었다. 제안된 시스템의 양자암호 키분배 관련 parameter는 전송거리 25km, 0.1 photon, 15% quantum efficiency(Dark Count Probability 8×10^{-5} c/gate) 조건에서 802bps의 R_{sift}, 9.4%의 QBER을 전송거리 50km에서는 606bps의 R_{sift}, 10.5%의 QBER을 나타냈다. 구현된 시스템은 50km까지 양자암호 키 분배가 가능하다. 시스템 광학

계의 정밀한 구성으로 visibility를 향상시킨다면 50km 이상의 장거리 전송이 가능할 것이다.

핵심되는 말 : 양자암호시스템, 위상안정화 광섬유, 양자키분배, 단일광자검출기

제 1 장 서 론

우리는 정보의 세상에 살고 있다. 예전부터 사람들은 마치 창과 방패처럼 다른 사람들이 읽을 수 없도록 메시지를 암호화 하였으며 또 다른 사람들은 이를 해독하려 했다. 예를 들어, 2차 세계대전 당시 독일인들은 독일의 암호기계였던 이니그마가 해독 불가능하다고 믿었으나 후에 이니그마의 암호문은 폴란드에 의해서 해독되었으며 후에 더욱 향상된 이니그마 역시 영국에 의해 해독되었다.[1] 이러한 정보 보안 문제는 현대에도 계속되어 인터넷을 비롯한 유무선 통신의 사용이 급속히 확대됨에 따라 국가, 기업, 금융상의 중요기밀 보호 및 개인의 사생활 보호 측면에서 그 중요성이 점점 더 증대되고 있다.

제 1.1 절 고전 암호체계

현대의 모든 암호체계는 대칭, 비대칭 암호체계로 나눌 수 있다. 대칭 암호체계는 앨리스와 밥 (암호학에서 보편적으로 쓰이는 전송자와 수신자를 말함)이 이브 (도청자)의 도청 가능성이 없는 가정하에 암호키를 서로 공유하는 것이며, 이 암호키는 암호화와 복호화에 쓰이게 된다. 이와 반대로 비대칭 암호체계는 한 쌍의 암호키를 사용하여 한 개는 암호화에 쓰고 다른 하나는 복호화에 쓰이게 된다.[9]

1.1.1 1회용 암호표 방식

1회용 암호표 방식은 1917년 AT&T의 Gilbert Vernam에 의해 개발 되었다.[3] 이는 대칭 암호체계에 속하며, 앨리스가 불규칙하게 생성된 암호키를 메시지에 더하여 암호화한 후 전송하면 밥은 수신한 메시지와 암호키의 차를 구해서 원본 메시지를 복호화 한다. 불규칙하게 생성된 암호키로 암호화된 메시지 역시 불규칙하

므로 이를 암호키 없이 복호화 하기는 불가능하다. 사실상 1회용 암호표 방식은 오늘날 완벽한 암호화 방식이다. 그러나 아래의 조건을 만족해야 한다.

1. 암호키는 불규칙하게 생성될 것
2. 메시지는 길어야 할 것
3. 단문에 대해서 한번만 사용 할 것

암호키는 불규칙하게 생성되어야 하며 메시지가 짧을 경우에는 불규칙한 경우라도 암호키를 알아내기 위한 경우의 수가 줄어들게 된다. 한 개의 암호키를 여러 문장에 사용하게 될 경우 이브는 암호문의 구조를 파악할 수 있게 된다. 예를 들어, 앨리스가 두 개의 문장에 같은 암호키를 두 번 사용하여 전송할 경우, 이브가 두 개의 서로 다른 암호화된 문장을 기록했다면 이 두 문장의 합은 암호화 되기 전의 원본 메시지가 된다.

이 암호 방식은 앨리스와 밥이 불규칙 생성을 위한 많은 양의 암호키를 이브의 도청 없이 안전하게 공유해야 한다는 단점이 있다. 암호키의 공유에 있어서 가장 안전한 방법은 아마도 앨리스와 밥이 서로 만나서 교환하는 것일 것이다. 이는 매우 비효율적인 방법이므로 다음과 같은 비대칭 암호체계가 개발 되었다.

1.1.2 공개키 방식

앞에서도 지적하였듯이 대칭 암호 체계의 가장 큰 문제점은 키분배의 어려움에 있다. 이를 극복하는 방안으로 스탠포드 대학의 Whitfield Diffie와 Martin Hellman은 공개키 방식라는 새로운 암호 모델을 1976 년에 제안했다.[2] 이 기술은 비밀키(private key)와 공개키(public key)라는 2개의 키쌍(key pair)을 구성해서 각 키가 암호화와 복호화에 사용되는 것을 의미한다. 비밀키는 소유한 사람 이외에는 절대로 알 수가 없는 키이고, 공개키는 누구에게나 공개된다. 공개키로 암호화하여 메시지를 보내고 나서 이를 비밀키로 복호화 하는 방식으로 메시지의 보안이 유지된다. 이 경우 밥은 하나의 키쌍만 가지고 복수의 앨리스로부

터 비밀 메시지를 받을 수가 있다. 공개키 방식은 대칭 암호체계에 비해 키관리는 편리하지만 알고리즘이 더 복잡한 이유로 처리속도가 더 걸린다. 메시지가 커질 경우 더욱 크게 증가하므로 공개키의 응용 분야는 Fig 1.2와 같이 비밀키로 암호화해서 메시지를 보내면 공개키로서 밥에서 암호를 해독하는 인증 모드(authentication mode)이다. 이 경우 메시지의 비밀성은 보장되지 않는다. 왜냐하면, 공개키는 누구든지 가질 수가 있으며, 이는 다시 말해서 누구든지 이 메시지를 읽을 수가 있다는 것을 의미하기 때문이다. 그렇지만 앨리스는 자신의 비밀키를 통해서 암호화했고, 밥은 비밀키에 해당하는 공개키로 메시지를 해독할 수 있기 때문에 앨리스는 받은 메시지가 밥으로부터 온 것임을 확신할 수가 있다. 결국 인증이라는 보안 서비스가 구현되며, 바로 이 특성이 디지털 서명의 기본 원리가 된다.

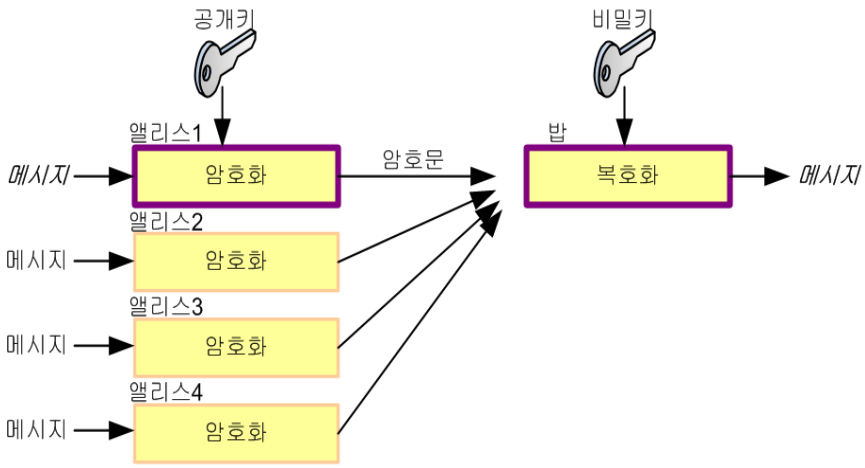

Fig 1.1 공개키 암호방식

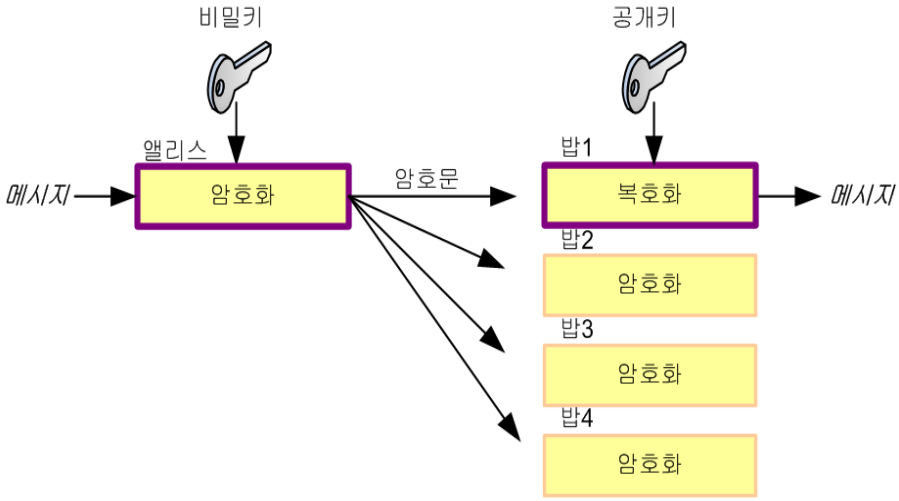

Fig 1.2 공개키 인증 방식

현재 널리 쓰이는 공개키 방식으로는 RSA가 있다. RSA는 MIT의 Rivest, Shamir, Adleman이라는 3사람 암호학자의 이름을 따서 만든 공개키 기반 암호 기술로서 현재 가장 널리 쓰이고 있다.[4] RSA는 수학적인 계산 복잡성에 기초한 암호체계로 현재 정교한 알고리듬의 발전에 따라 그 안전성에 의문이 제기되고 있으며, 1994년 AT&T의 Peter Shor가 양자컴퓨터를 이용한 소인수분해 알고리듬을 개발함으로써 양자컴퓨터가 개발되면 RSA 암호체계는 근본적으로 해독이 가능한 것으로 판명되고 있다.[5][6] 결국 절대 보안이 유지되는 암호 방식은 1회용 암호표 방식이며 여기서 암호키 분배의 문제는 양자암호로 해결 할 수 있게 된다.

1.2 절 양자암호

양자암호는 1970년대 Stephen Wiesener가 제안한 복제 불가능한 “quantum money"에서 시작된다[7]. 이 아이디어는 두 개의 비직교 편광 기반을 갖는 광자를 돈에 저장한다는 것이다. 그래서 돈을 복제하려는 사람은 복제하기에 앞서 돈에 저장된 광자의 상태를 측정해야 한다. 그러나 복제하려는 사람은 돈에 저장된 광자의 기저를 모르기 때문에 측정할 때 일정한 확률로 에러가 나오게 된다. 이렇게 잘못된 상태로 저장된 복제된 돈은 은행에서 가지고 있는 올바른 기저상태로 측정하게 되면 복제 여부를 쉽게 알 수 있게 된다. Wiesener의 제안은 그 당시 획기적인 것이었지만, 광자를 오랜 시간동안 저장할 수 없다는 이유에서 여러 과학 저널에서 게제 거절을 당했다. 그러나 1984년 Charles Bennett 과 Gilles Brassard 는 "Quantum money"의 아이디어에서 광자를 저장하지 않고 Quantum channel 을 통해 전송을 하자는 제안을 했고 이것이 양자암호가 개발된 배경이다.[7]

1984년 제안된 양자암호는 1989년 Bennett 등에 의해 처음으로 실험으로 증명되었고 1992년 그 결과가 발표되었다.[8] 양자암호는 양자채널의 종류에 따라 광섬유를 이용하는 방식과 대기 중을 이용하는 방식으로 나눌 수 있다. 이 두 가지는 원리적으로는 서로 같으나 응용 분야나 전송 효율을 증대하기 위해 알맞은 파장대 등의 차이점이 있다. 대기 중을 통한 양자암호통신은 투과 손실이 적은 770nm 대역의 광원을 사용하며 이 대역에서 Si APD를 사용하게 되면 60%~70% 의 높은 양자효율을 얻을 수 있는 장점이 있다.[9] 대기 중을 통한 양자암호통신은 특히 위성과 지상 사이의 암호통신에 응용할 수 있다는 것이 장점이나 거리가 늘어남에 따라 신호가 공간적으로 퍼지는 문제, 날씨 등의 영향을 많이 받는 다는 점에서 단거리 암호통신에 제한된다. 대기 중을 통한 양자암호 실험은 2002년 독일에서 23.4 km 양자채널과 100bps의 키 전송속도 실험이 보고되었다.[10]

광섬유를 이용하는 방식은 기존의 광통신에서 표준으로 사용되고 있는 단일모드 광섬유를 사용하여 1550nm 대역에서 손실이 0.2dB/km 정도로 낮은 장점을 이용하여 장거리 양자암호시스템 구현에 적합하다. 그러나 분산, 편광의 변화, PMD,

기타 다양한 광섬유 전송상의 비선형 효과들은 양자암호통신 시스템의 성능을 떨어뜨리게 된다. 현재 이 문제점을 해결하기 위해 다양한 연구가 진행 중이며 10bps 의 낮은 전송속도이지만 최고 122km 의 전송거리를 갖는 연구도 보고 되었다.[11] 아래 Table 1.1은 주요 양자 암호 실험을 나타낸다.[12]

연구기관	국가	기술내용	성능			발표 년도	참고문헌	비고
			키 생성속도	거리	QBER			
IBM(C.H. Bennett)	미국	Free air channel Polarization coding	10bps	30cm	–	1992	J. Cryptology, vol.5, p.3	최초의 양자 암호 실험
BT Lab.(P. Townsend)	영국	Multi-user, 1X3 PON system	1kbps	5.4km	3%	1997	Nature, vol.385, p.47	다중 사용자, PON 구조
Los Alamos Lab. (R. Hughes, C.G. Peterson)	미국	Double Mach-zehnder type Installed fiber channel	10bps	48km	9.3%	2000	J. Mod. Opt. vol.47, p.533	
Universität Wien (A. Zeilinger)	오스트리아	Entangled photon pairs Polarization coding 700nm fiber channel	420bps	500m	3.4%	2000	Phys. Rev. Lett. vol.84, p.4729	
University of Geneva (N. Gisin)	스위스	Entangled photon pair energy-time coding 1310nm fiber channel	33bps	20km	4%	2000	Phys. Rev. Lett. vol.84, p.4737	
Heriot-Watt University (G. Buller), Corning Research Centre(P. Townsend)	영국	Spatial multiplexing 1550nm fiber channel	–	80km	9%	2001	J. Mod. Opt. vol.48, p.1957	
Defence Evaluation and Research Agency(J. Rarity, P. Gorman, P. Tapster)	영국	Polarization coding free space channel	685bps	1.9km	5.1%	2001	Elec. Lett. vol.37, p.512	
University of Geneva (N. Gisin)	스위스	Plug & Play system 1550nm fiber channel	44bps	67.1km	6.1%	2002	New J. Phys. vol.4, p.41	Plug & Play
Mitsubishi Electric	일본	1550nm fiber channel between Tokyo and Mt. Fuji	7.2bps	87km	7.6%	2002	Mitsubishi Electric Report	
Ludwig-Maximilian University(H. Weinfurter)	독일	Polarization coding Free space channel	hundreds bps	23.4km	–	2002	Nature vol.419, p.450	
Los Alamos Lab. (R. Hughes, C.G. Peterson)	미국	Free air channel in daylight Polarization coding	651bps	10km	3.2%	2002	New J. Phys. vol.4, p.43	
IBM(D. Bethune, W. Risk)	미국	Autocompensating type Phase coding	200bps	20km	3%	2002	New J. Phys. vol.4. p.42	
BBN, Harvard, Boston University(G. Troxel)	미국	Quantum Network Standard telecom fiber	1kbps	10km	6~8%	2003	quant-ph/0307049	VPN 기반 테스트베드 구축
Telcordia Technologies (M. Goodman), Los Alamos Lab.(R. Hughes)	미국	1300nm data signal 1550nm sync signal	91bps	10km	–	2003	IEEE Photonics Tech. Lett. vol.15, p.1669	
l'Institut d'Optique (P. Grangier), Université Libre de Brux(N. Cerf)	프랑스 벨기에	Continuous variable QKD	470kbps	tabletop	–	2003	Nature, vol.421, p.238	연속변수 이용
Toshiba Research Europe (A.J. Shields)	영국	Plug & Play system 1550nm fiber channel	9.2bps	122km	8.9%	2004	App. Phy. Lett. vol.84, p.3762	

연구기관	국가	기술내용	성능			발표 년도	참고문헌	비고
			키 생성속도	거리	QBER			
NEC, ERATO (K. Nakamura)	일본	PNP system 1550nm fiber channel	–	150km	–	2004	Jpn. J. Appl. Phys. vol.43, L1217	단순한 간섭 현상 확인 실험
NIST(C.J. Williams)	미국	845nm free space channel, 1.25Gbps clock sync.	1Mbps	730m	1.1%	2004	Opt. Express, vol.12, p.2011	
University of Geneva (N. Gisin)	스위스	Energy-time entanglement Standard telecom fiber	23bps	30km	10.5%	2004	Eur. Phys. J. D, vol.30, p.143	양자 얽힘 광원
Heriot-Watt University (G. Buller) University College Cork (P. Townsend)	영국 아일랜드	Polarization coding B92 1300nm fiber channel GHz clocked	7kbps	10km	2.1%	2004	IEEE J. Q. Elec. vol.40, p.900	
Northwestern University (H.P. Yuen, P. Kumar)	미국	Coherent state의 양자 잡음을 이용하는 방법, Yuen protocol	650Mbps	200km	–	2005	Phys. Rev. vol.71, p.062326	프로토콜의 안전성 미검증
NTT, Stanford University (Y. Yamamoto)	일본 미국	Differential phase shift QKD	209bps	105km	7.95%	2005	quant-ph/0507110	DPSK 방법

Table 1.1 주요 양자암호 실험

제 2 장 양자암호 프로토콜

양자암호 프로토콜은 양자암호키 분배를 위해 앨리스와 밥 사이에 정해진 일종의 규약이다. 이 규약을 통해 앨리스와 밥은 양자암호키를 생성하며 대표적인 프로토콜로 BB92, BB84가 있다.

제 2.1 절 BB84 프로토콜

최초의 양자암호 프로토콜은 1984년 IBM의 C.H. Bennett 과 몬트리올 대학의 G. Brassard에 의해 제안 되었다.[7] 제안자들의 이름을 따서 BB84 프로토콜로 명명되었으며 두 개의 비직교 기저를 이루는 네 개의 양자 상태를 이용한다.

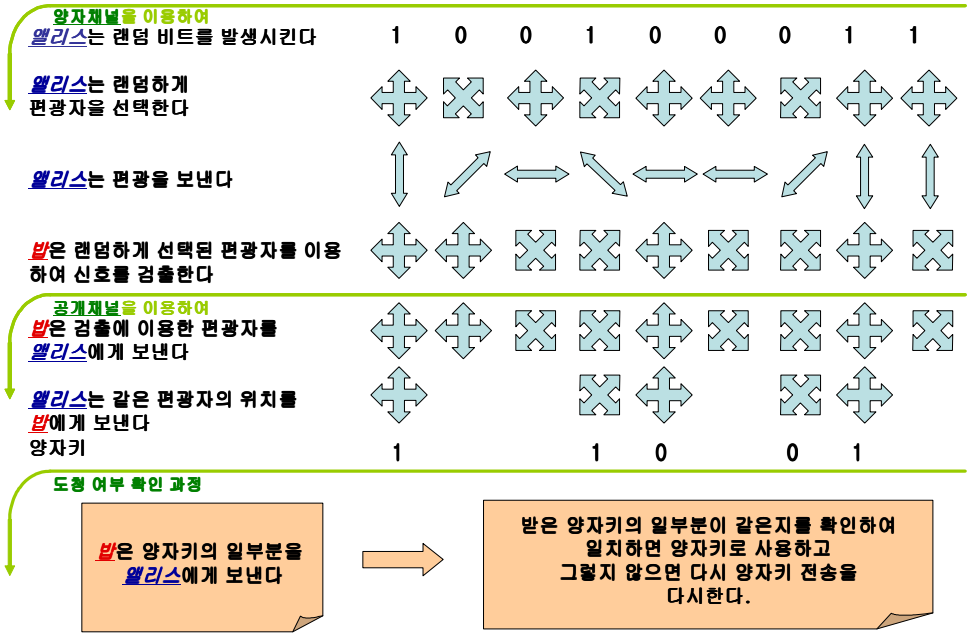

Fig 2.1 BB84 프로토콜

Fig 2.1은 BB84 프로토콜의 절차를 나타낸다. 앨리스에서 4개의 양자 상태를 불규칙하게 생성하여 이의 한정된 연속신호를 양자채널을 통해서 밥에게 전송한다. 밥은 마찬가지로 불규칙하게 2개의 기저중 한 개를 선택하여 앨리스에서 전송된 연속신호를 측정한다. 앨리스는 자신이 어떠한 기저를 사용하여 신호를 생성했는지 공개 채널을 통해서 밥에게 알려준다. 앨리스와 밥은 올바른 기저를 선택한 신호만을 사용하게 되며 다른 기저를 사용한 신호는 버리게 된다. 이렇게 마지막으로 생성된 신호는 공개채널을 통해 그 신호의 일부분을 공개한다. 그리고 앨리스와 밥은 이를 다시 비교하여 이브가 존재하는 지를 검사하게 된다. 이브의 도청 시도가 없다고 판단되면 나머지 신호를 암호키로 사용하게 된다. 이를 요약하면 아래와 같다[2].

1. 앨리스는 4개의 편광된 양자 상태를 불규칙하게 생성하여 밥에게 보낸다. (양자채널)
2. 밥은 불규칙하게 생성된 기저를 통해 수신된 양자 상태를 측정한다. (양자채널)
3. 밥은 앨리스에게 사용한 기저의 정보를 알려준다. (공개채널)
4. 앨리스는 자신의 기저와 밥의 기저가 같은 신호열의 위치를 알려준다. (공개채널)
5. 앨리스와 밥은 같은 신호열의 정보만을 저장하며 나머지는 버린다.
6. 앨리스와 밥은 저장된 정보의 일부분을 공개, 비교하여 오류의 비율을 계산하여 이브의 도청 여부를 판단한다. (공개채널)
7. 이브의 도청이 없을 경우 양자키로 사용하며 이브의 도청이 있을 경우는 다시 프로토콜을 수행한다.

아래의 Fig 2.2에서 보듯이 만약 이브의 도청이 있다면 앨리스와 밥이 같은 기저를 사용했더라도 다른 정보를 갖게 될 경우의 수가 생긴다. 양자암호에서 이는 에러로 인식된다. 실제로 에러율은 양자암호 시스템의 광학계 구성에 의한 노이즈와 단일광자검출기에서의 노이즈 등에 의해 이브의 도청이 없이도 일정값이 생기

게 된다. 이브의 도청이 있다면 에러율이 앞에서 언급한 노이즈가 있음에도 불구하고 현저하게 높아질 것이며 이를 근거로 이브의 도청 유무를 판단하게 된다. 최종적으로 생성된 양자키는 여러 가지 노이즈가 포함되어 있다. 다시 말해서 이브의 도청이 없이도 같은 양자키를 갖을 수 없게 된다. 이는 여러 가지 에러 정정 방법을 통해서 해결하게 된다.[13]

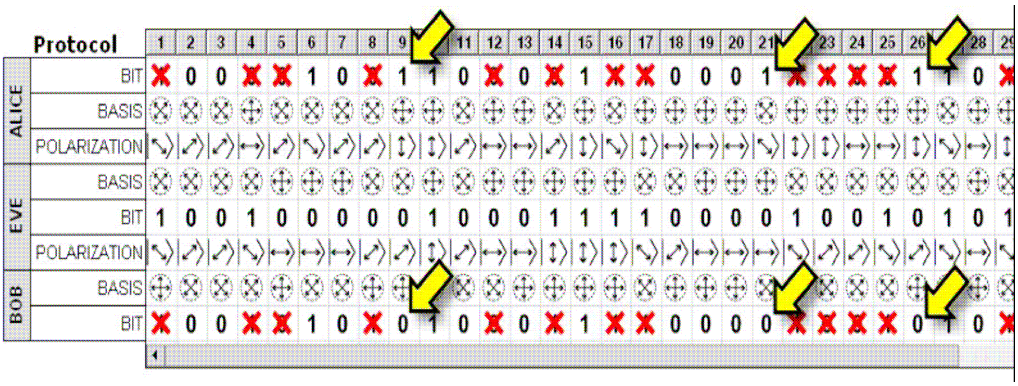

Fig 2.2 BB84 프로토콜에서 이브의 도청 유무 판별

제 2.2 절 BB92 프로토콜

1992년 Bennett은 좀 더 간단한 양자암호 프로토콜을 제안하였다.[26] Fig 2.3에서와 같이 앨리스는 밥에게 보낼 0과 1의 불규칙 신호를 만들고, 0은 ↔, 1은 ↗의 편광을 보낸다. 밥도 불규칙 신호를 만들어, 0은 ↖, 1은 ↕의 편광판으로 측정을 한다. 앨리스와 밥의 신호가 같은 50%의 경우에 편광과 편광판이 45도 겹치므로, 50%의 확률로 단일광자를 검출할 수 있다. 두 사람의 이진수가 다를 경우에는 편광과 편광판의 방향이 수직이 되어서 Bob은 광자를 검출할 수 없다. 따라서 이 방식으로는 전체적으로 25%의 확률로 밥이 단일광자를 검출하게 되고, 이들 경우만 밥이 앨리스에게 알림으로써 두 사람은 같은 이진난수열을 가지게 된다. 또한, 두 사람은 마찬가지로 BB84 프로토콜에서처럼 공개된 채널을 통해 일부 데이터를 비교함으로써 채널의 신뢰도 및 도청 여부를 판별할 수 있다.

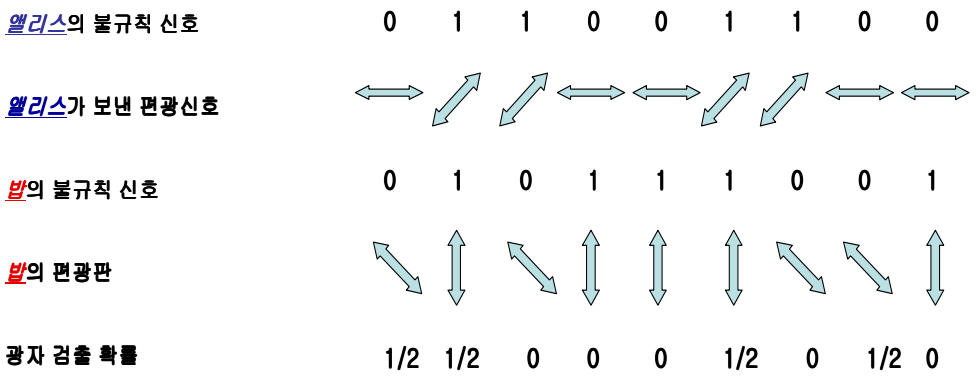

Fig 2.3 BB92 프로토콜

제 3 장 양자암호시스템 구현

양자암호시스템은 구현 방법에 따라서 몇 가지로 나눌 수 있는데 크게 편광 코딩 기반과 위상 코딩 기반 그리고 plug & play 시스템으로 나눌 수 있다.

제 3.1 절 편광 코딩 시스템

편광 코딩 시스템은 Fig 3.1 와 같이 구성된다. 앨리스의 시스템은 4개의 레이저 다이오드로 구성되며 각각의 광원은 -45°, 0°, +45° 그리고 90°의 편광을 갖게 된다. 정해진 편광에 따라 4개의 레이저 중에 한 개가 동작을 하게 되며 광원은 필터에 의해 단일 광자 이하로 감쇄되어 전송된다. 편광 모드 분산에 의해서 광신호의 편광은 변하게 되고 마찬가지로 이로 인해 지연이 생기게 되므로 밥에 전송되기까지 편광은 유지 되어야 한다. 광섬유를 통해 전송된 광신호는 waveplate를 지나게 되어 원래의 편광을 유지하게 되며 beamsplitter를 지나게 된다. polarization beamsplitter에서 직교 기저와 대각 기저를 이용하여 측정을 하게 되며 이는 APD에 검출된다[9].

+45° 편광된 신호를 생각해보면, 광섬유를 지나게 되면서 편광은 변하게 된다. 변화된 광신호는 밥의 입력부분에 있는 waveplate에서 변이된 편광을 보정해주며 beamsplitter를 지나 만약 직교 기저의 PBS로 광원이 가게 된다면 50%의 확률로 “1” 또는 “0”의 APD에 검출 될 것이다. 만약 beamsplitter를 지나 대각 기저의 PBS로 가게 된다면 PBS는 광신호를 반사하여 “0”의 APD에 검출 될 것이다. 앨리스의 4개의 레이저 다이오드와 밥의 2개의 PBS는 Pockels cell과 같은 능동 편광 변조기를 사용해도 된다[15].

Geneva 대학의 Antoine Muller는 광섬유 양자 채널을 이용하여 상기 시스템을 실험하였다[16]. 800nm 파장을 이용하여 1.1km를 전송하였으며 1310nm 파장대를 이용하여 23km 양자 전송 채널에서 양자키 전송을 성공하였다[17][18]. 이는 실험

실이 아닌 외부 환경에서의 양자암호 최초의 실험이었으며 Swisscom 전화 회사의 optical fiber 전송선을 양자 채널로 사용했다.

상기 두 실험에서 광섬유를 이용하여 편광된 광신호를 보내는 방법은 오랜 시간동안 편광이 안정적이지 못하고 계속 변하는 것을 확인할 수 있었다. 이는 시간이 지날수록 시스템에서 능동적으로 편광을 정렬 시켜주어야 함을 의미한다. James Franson은 위와 같은 문제점을 해결하기 위해 active feedback alignment system을 이용하여 양자암호를 구현했으나 키 전송에는 문제가 있었다[19]. 능동적으로 편광을 보정해주는 방법은 몇 가지가 있다[20]. 편광 유지 광섬유의 이용은 그 방법 중 하나가 될 수 있다. 그러나 편광유지광섬유(Polarization maintaining fiber)를 양자 채널에 이용하는 것은 문제가 있다. 실제적으로 편광유지광섬유는 이상적으로 편광을 유지 시키지 못하기 때문이다. 이러한 문제점으로 광섬유는 양자암호 전송 채널로 적합하지 않다. 그러나 양자 채널이 자유 공간이라면 이 문제는 해결 된다.

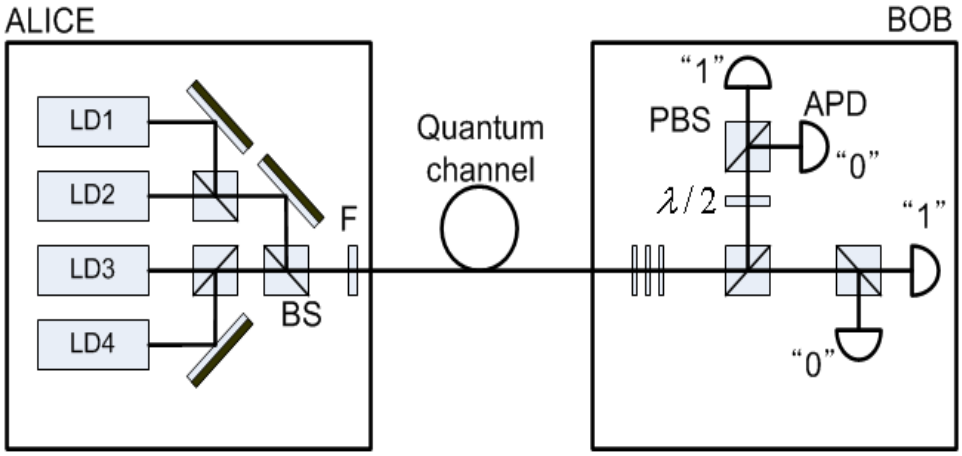

Fig 3.1 편광 코딩 양자암호 시스템

(LD: laser diode, BS: beamsplitter, F: filter for attenuation, PBS: polarization beam splitter, $\lambda/2$: half waveplate, APD: avalanche photodiode)

제 3.2 절 위상 코딩 시스템

3.1절에서 살펴본 바와 같이 편광 코딩 시스템에서 편광 변화는 시스템 구현에 큰 단점으로 작용하였다. 이의 해결책으로 Bennett은 BB92 프로토콜을 제안할 당시 광자의 위상에 코딩하는 방식을 처음으로 제안하였다. 이 시스템은 간섭계를 기본 구조로 하여 단일모드광섬유를 사용하였다[9]. Fig 3.2는 광섬유를 이용한 Mach-Zehnder 간섭계이다.

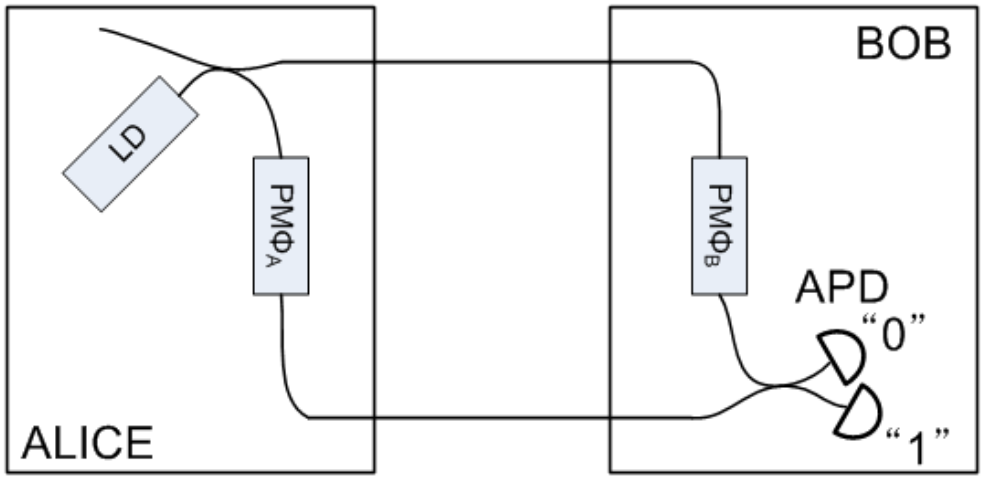

Fig 3.2 Mach-Zehnder 간섭계

(LD: laser diode, PM: phase modulator, APD: avalanche photodiode)

간섭계는 길이가 같은 2개의 beamsplitter를 대칭으로 연결하여 구성된다. 앨리스에는 레이저 다이오드와 한 쪽 경로에 위상변조기 PMϕ_A이 위치하게 되며 밥은 마찬가지로 한 쪽 경로에 위상변조기 PMϕ_B와 2개의 APD로 구성된다. 간섭계의 정렬은 간섭 신호에 중요한 영향을 주므로 레이저를 continuous 모드로 동작하여 출력 신호를 관찰함으로서 시스템의 정렬 상태를 확인할 수 있다. 두 광신호의 coherence length는 반드시 간섭계 두 경로의 차이보다 커야 한다.

Beamsplitter에서 반사될 경우 위상 변화 $\pi/2$를 고려했을때, 위상변조기를 이용한 위상 변화 ϕA, ϕB와 , 광섬유의 두 경로차 ΔL에 의한 "0" 포트 APD의 출력의 크기는 식 3-1과 같다.

$$I_0 = \bar{I} \cdot \cos^2(\frac{\phi_A - \phi_B + k\Delta L}{2}) \qquad (3\text{-}1)$$

k는 파동수, I는 광원의 세기를 나타낸다. 만약 위상 값이 $\pi/2 + n\pi$ 이면 (n은 정수) out of phase로 상쇄 간섭이 발생하여 "0" 값을 갖는 APD의 출력 신호는 최소값이 나오게 되고 "1" 값을 갖는 APD의 출력 신호 세기는 최대값이 나오게 된다. 만약 위상 값이 $n\pi$ 이면 in phase로 보강 간섭이 발생하게 되며 상쇄 간섭과는 반대로 APD 출력신호를 갖게 된다. 간섭계는 광학 스위치와 같이 작동하게 되며 안정적인 간섭 신호를 얻기 위해서는 간섭계의 두 경로차가 안정적으로 유지 되어야 한다.

이전까지는 일반 광원으로 간섭계의 특성을 설명하였다. 간섭계의 특성은 단일광자를 사용하여도 일반 광원을 사용했을 때와 마찬가지의 특성을 보이게 되며 앨리스와 밥의 위상 변조값에 따라 APD 출력 신호를 스위칭 할 수 있다.

검출시 광원은 입자의 성질을 가지게 되지만 간섭계에서 전송시에는 파동의 성질을 갖게 된다. 이는 Young's double slit 실험에서 관찰할 수 있는데, Mach-Zehnder 간섭계는 광섬유를 이용한 double slit 실험과 같다. 이 간섭계는 양자암호키 전송을 위해 단일광자검출기와 단일광자소스에 연결된다. 앨리스는 단일광자 소스, coupler, 위상변조기로 구성이 되며 밥은 위상변조기, coupler, 검출기로 구성된다. BB84 프로토콜을 적용해보면, 앨리스는 비트를 인코딩하기 위해 4가지 상태의 위상 변화값(0, $\pi/2$, π, $3\pi/2$) 중에 하나를 선택하여 변조하게 된다. 0, $\pi/2$ 변조값은 비트 "0"으로 π, $3\pi/2$ 변조값은 비트 "1"으로 인식한다. 반면에 밥은 BB84 프로토콜에서 대각, 직교 기저를 불규칙하게 선택하게 되는데 위상 변조값 0, $\pi/2$ 가 이에 해당된다. 밥은 비트 "0"으로 인식하는 port 0에 그리고 비트 "1"으로 인식하는 port 1에 광자검출기에 연결된다. 앨리스와 밥의 위상 변화 차이에 의해서 검출 port가 정해지며 동시에 변조값과 검출값이 저장된다. 밥은 검출값을 확인하고 자신의 변조값과 비교하여 앨리스의 변조값을 추론한다.

BB84 프로토콜을 사용하여 추론 가능한 모든 위상 변조의 경우는 Table 3.1과 같다.

Alice		Bob		
Bit value	φ_A	φ_B	φ_A-φ_B	Bit value
0	0	0	0	0
0	0	π/2	3π/2	?
1	π	0	π	1
1	π	π/2	π/2	?
0	π/2	0	π/2	?
0	π/2	π/2	0	0
1	3π/2	0	3π/2	?
1	3π/2	π/2	π	1

Table 3.1 BB84 프로토콜을 사용한 위상 변조 코딩

암호키 분배 중에는 반드시 간섭계의 안정성이 확보 되어야 한다. 간섭계의 경로차가 광자 파장의 1/2 이상으로 변하게 되면 간섭된 신호는 다른 port로 향하게 되며 이는 에러로 연결된다. 경로차의 발생 원인은 두 경로의 온도 변화의 차이 또는 광섬유의 진동과 같은 물리적인 변화 등에 있다. 비록 실험실 광학 테이블에서는 안정된 간섭을 유지할 수 있을 지라도 양자 채널 전송 거리를 몇 미터만 늘리게 되면 간섭의 안정성 확보는 사실상 불가능하다. 그래서 Bennett은 Fig 3.3의 시스템으로 이 문제를 해결했다[8]. 그는 두 개의 비대칭 Mach-Zehnder 간섭계를 양자 채널을 사이에 두고 연결하는 방식을 사용했다.

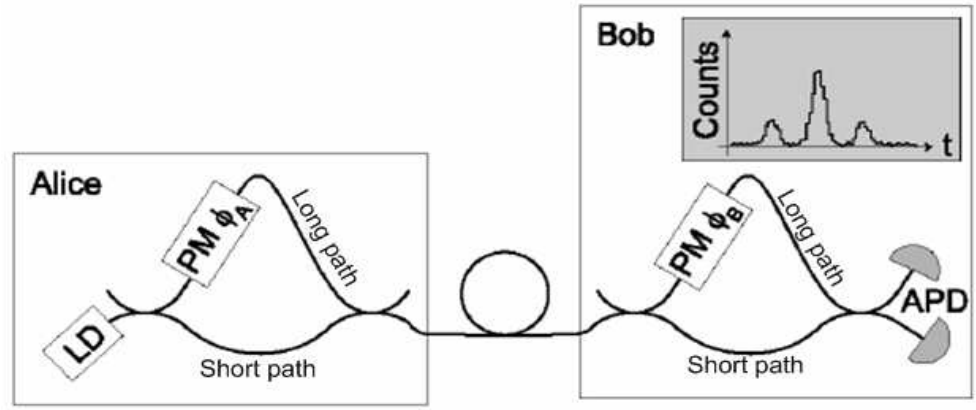

Fig 3.3 비대칭 Mach-Zehnder 갑섭계를 이용한 시스템
(LD: laser diode, PM: phase modulator, APD: avalanche photodiode)

밥에서 검출된 광신호를 시간에 따라 측정하게 되면 3개의 신호를 검출할 수 있다. 첫 번째 신호는 short(Alice) - short(Bob) path를 지나 검출된 신호이며 세 번째 신호는 long(Alice) - long(Bob) path를 지나 검출된 신호이다. long - short path 와 short - long path를 지나는 두 신호는 서로 간섭되어 두 번째 신호로 검출 된다. 양자암호 키 분배에서는 첫 번째와 세 번째 신호는 무시하며 두 번째 신호에 타이밍 윈도우를 사용하여 간섭 신호를 확인한다.

이 시스템의 장점은 앨리스에서 전송되는 두 광신호가 양자 채널에서 같은 경로를 지난 다는 것이다[9]. 그래서 앨리스와 밥의 short, long arm 부분에만 길이가 같도록 해주면 된다. 이는 Fig 3.2의 시스템보다 안정성 구현에 있어서 용이하다. 밥에서 검출 되는 3개의 펄스 간격은 서로 구별 가능할 수 있도록 충분히 떨어져야 된다. 펄스 간격은 펄스 width 보다 커야 하며 광자검출기에서의 타이밍 지터보다 커야 한다. 만약 타이밍 지터가 500ps이면 펄스의 간격은 최소한 1.5ns 이상 유지 되어야 한다.

이 시스템의 단점은 이전 시스템에서처럼 키 분배를 하는 중에 간섭되는 두 신호가 1/2 파장 안에 유지 되어야 하는 것이다[21]. 이는 온도가 안정적으로 유지되는 박스 안에 광학 부품을 구성하고 정밀한 능동 온도 제어기를 통해 온도를

제어해야 함을 의미한다. 또한 short, long arm의 편광 변화도 고려하여 이를 편광 제어기로 보정해야 한다.

DERA의 Paul Tapster 와 John Rarity 는 1993년 10km 양자 채널에서 비대칭 Mach-Zehnder 간섭계를 이용한 양자키 전송 실험을 하였다[22]. 후에 Paul Townsend 연구진은 이 시스템에 polarization beam splitter를 이용하여 시스템을 구성하여 실험 하였으며 에러 신호를 최소화 하였다[23][24][25]. 또한 하나의 전송 채널을 추가하여 양자키를 인코딩한 데이터를 전송하는 시스템을 실험하기도 했다.

제 3.3 절 Plug & Play 시스템

3.3.1 Plug & Play 시스템

3.2 절에서 설명한 시스템은 간섭의 안정성과 편광의 보정 등을 위해서 정밀한 능동 제어 기술이 필요하다고 언급했다. 능동 제어 기술은 1989년 Martinelli에 의해 처음 제안되었는데, 능동 또는 수동으로 위상 변화와 편광 변화를 보정해주고 있다[26]. 제안된 시스템은 Fig 3.4와 같다.

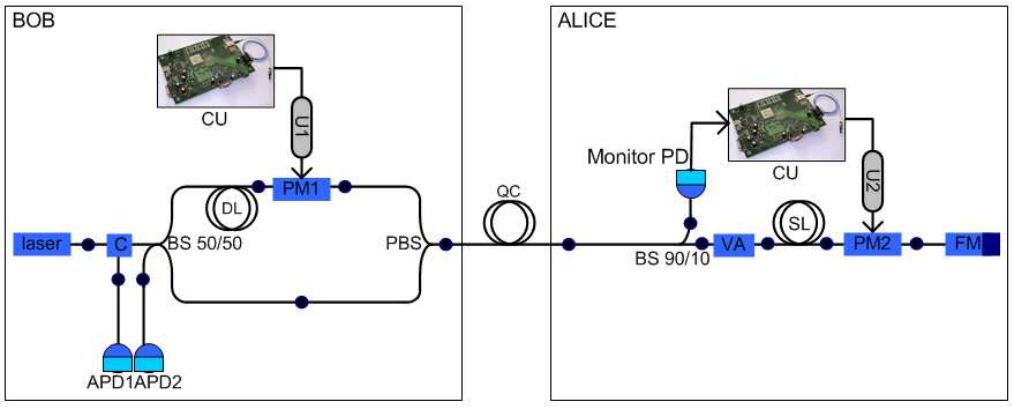

Fig 3.4 Plug & Play 시스템 광학부

(C: circulator, APD: avalanche photodiode, BS: beamsplitter, PM: phase modulator, PBS: polarization beamsplitter, DL: delay line, QC: quantum channel, PD: photo detector, VA: variable attenuator, SL: storage line, FM: faraday mirror)

밥의 광학 구성은 레이저 다이오드, circulator, avalanche photodiode, beamsplitter, phase modulator, polarization beamsplitter, polarization maintaining optical fiber 의 광학 부품으로 구성된다. 앨리스의 구성은 9:1의 비율을 가진 beamsplitter, photo detector, variable attenuator, phase modulator,

faraday mirror로 구성된다.

일반적인 양자암호 시스템은 광신호를 앨리스에서 전송하여 밥에게 전달된다. 그러나 Plug & Play 시스템은 광신호를 밥에서 앨리스로 전송하며 faraday mirror에서 반사되어 다시 밥에게 되돌아 간다. 광학 부품의 역할과 함께 시스템을 살펴보면, 레이저 다이오드에서 레이저 펄스 신호를 보내면 circulator를 지나 BS1으로 가게 된다. circulator는 port1, port2, port3 세 개의 포트로 구성이 되며 port1로 들어간 빛은 port2로 port2로 들어간 빛은 port3로 전달해주는 스위칭 역할로 되돌아 오는 빛을 APD로 전달해주는 passive switching을 한다. 밥의 모든 광섬유는 단일모드 편광유지광섬유를 이용한다. BS1을 지난 빛은 50:50으로 나뉘어 long arm 과 short arm의 두 경로로 나뉘어 진다. short arm을 지나는 빛은 PBS를 지나 양자 채널로 향하게 되며 long arm을 지난 빛은 phase modulator와 DL을 거쳐 PBS로 향하게 된다. 이때 phase modulator는 동작하지 않아야 하며 DL으로 인해서 그 거리만큼 short arm을 지나는 신호와 시간 지연이 생긴다. 또한 long arm을 지나는 신호는 PBS의 pigtail fiber가 orthogonal하게 꼬여 있어 PBS를 나올 때는 원래의 편광 보다 90° 변하게 된다. 결국 PBS를 지나서는 DL 만큼의 시간 지연을 갖는 두 개의 펄스가 나오게 되며 이 두 신호는 서로 직교한다. 이 두 신호는 양자 채널을 통해 앨리스에게 전송된다. 앨리스에 전송된 두 신호는 BS9/1을 지나 광신호의 90%는 D1으로 가게되며 나머지 10%는 VA로 가게 된다. D1의 역할은 밥에서 전송된 광신호를 인식하는 역할을 한다. 만약 D1이 없다면 언제 밥에서 신호가 오는지 모르게 된다. 인식된 타이밍에 맞춰 VA와 PM2를 정확한 타이밍에 동작하게 된다. 광신호 세기가 10% 비율로 줄어든 두 신호는 VA를 지나게 되며 SL과 PM2를 지나 FM으로 향하게 된다. faraday mirror는 두 신호를 orthogonal 하게 편광을 바꿔주는 동시에 반사한다. 결국 FM을 지나기 전과 후의 신호는 90°만큼 편광이 바뀌게 된다. 반사된 신호는 PM2를 다시 지나게 되며 두 신호 중에 뒤에 따라오는 신호를 위상 변조하게 된다. phase modulator는 보통 전기광학 변조기를 사용하게 되는데 이때 변조기에 전달되는 전기 신호는 rising time 과 falling time이 짧아야 한다. 그래야 두 광 신호 중 한 개의 신호만 위상 변조를 할 수 있다. 두 신호는 SL을 지나게 되며 VA를 지나게 되어 단

일 광자의 에너지만큼 감쇄시켜준다. SL의 역할은 뒤에 설명하겠다. 두 신호는 밥으로 되돌아가며 앨리스의 PBS를 지나게 된다. PBS의 역할은 Fig 3.5와 같다.

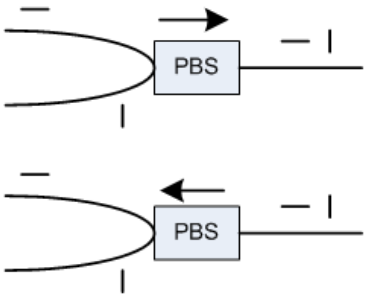

Fig 3.5 PBS의 역할

PBS와 faraday mirror 때문에 결국 short path를 지났던 신호는 되돌아 오면서 long path로 향하게 되며 long path를 지나던 신호는 되돌아 오면서 short path로 향하게 된다. 이때 long path를 지나는 신호는 PM1에 의해서 위상 변조된다. 하나의 신호는 앨리스에서 나머지 하나는 밥에서 위상 변조가 된다. 두 신호는 BS1에서 간섭을 하게 되며 두 신호의 위상 차이에 따라 보강 간섭과 상쇄 간섭이 결정된다.

Plug & Play 시스템은 신호가 왕복으로 되돌아오는 시스템으로 광섬유에서 전송되면서 backscattering이 일어난다. backscattering 신호는 밥에 전송되어 APD에서 에러로 검출될 수 있다. 이런 이유로 밥은 레이저를 pulse train으로 동작하여 앨리스에게 보내게 되며 앨리스는 SL에서 pulse train을 일정 시간동안 저장하여 backscattering 신호를 없앤다. SL은 보통 수십 km의 길이를 가진 광섬유이다. 밥은 pulse train이 도착하기 전까지 다음 pulse train을 전송하지 않고 기다린다. 광학부를 구성함에 있어서 중요한 점은 BS1, PM1, PBS 사이의 모든 port의 편광축을 정확히 맞춰야 한다. PM1에서 나오는 신호는 편광축을 조정하여 최대의 신호가 나와야 하며 short path의 PBS의 커넥터를 조정하여 마찬가지로 최대의 신호가 나와야 한다. 만약에 편광축이 맞지 않는다면 최종적으로 밥에서 신호를 관측했을때 주변에 에러 신호가 나오게 되며 결국 두 간섭될 신호의 크기 차이도 생기게 되어 visibility에 영향을 주게 된다.

3.3.2 Prototype Setup

Prototype Setup 은 Quantum channel을 이용하여 1550nm 파장에서 양자키 분배를 위해 단일광자 전송을 하며 1310nm 파장에서 10~100 광자를 전송하여 양자키로 암호화 된 데이터 교환에 이용한다. 이를 구분하기 위해 Wavelength Division Multiplexer (WDM)을 사용하며 시스템 구성은 Fig 3.6, 3.7과 같다.

Fig 3.6에서 Laser1은 500ps의 짧은 펄스 width를 갖는 1550nm 파장의 다광자 레이저 신호를 발생하며 TL1에 의해 current drive된 열전소자에 의해 온도 안정화되어 있다. 이는 1550nm 파장의 안정성을 확보하기 위해서다.

Laser1의 pigtail 광섬유는 Polarization Maintaining fiber로 pigtail된 circulator C1에 연결되며 이는 rotatable FC 커넥터를 사용한다. 레이저에서 나오는 광신호의 편광축과 C1 PMF의 편광축을 맞추기 위해 FC 커넥터를 회전하여 조정한다. C1은 BS50/50에 연결되며 BS50/50에 의해 하나의 광신호는 2개의 광신호로 분리되며 분리된 신호는 PBS와 PM1으로 구성된 Mach-Zehnder 간섭계로 입사된다. 레이저를 시작으로 Mach-Zehnder 간섭계까지의 모든 광섬유는 PM 광섬유를 사용한다. Mach-Zehnder 간섭계는 current drive(Fig 3.6에서 T)하여 TEC를 이용하여 온도 안정화 한다. PM1은 U1에 의해 0과 π/2의 위상값에 해당하는 50ns width의 펄스 신호를 인가하게 된다. PBS를 나온 두 광신호는 WDM1을 지나 1~50km의 길이를 가진 QC를 지나게 된다.

Single Photon Counter는 낮은 dark current를 유지하기 위해 geiger mode로 동작하는 APD1과 APD2로 구성된다. Geiger mode 펄스 신호는 2~5ns의 width, breakdown 전압에서 5~10V 높은 Amplitude를 갖게 된다. APD1,2 출력 신호는 증폭기를 이용하여 TTL 레벨의 신호로 변환한다(Fig 3.6에서 A1, A2). Dark current는 current drive(Fig 3.6에서 TA1, TA2)하여 구동되는 TEC에 의해 약 -50℃로 냉각된다. Circulator (C2, C3)에 연결된 WDM과 storage line(SL, 25km)의 길이를 제외하고는 Gisin 연구진의 setup과 동일하다.

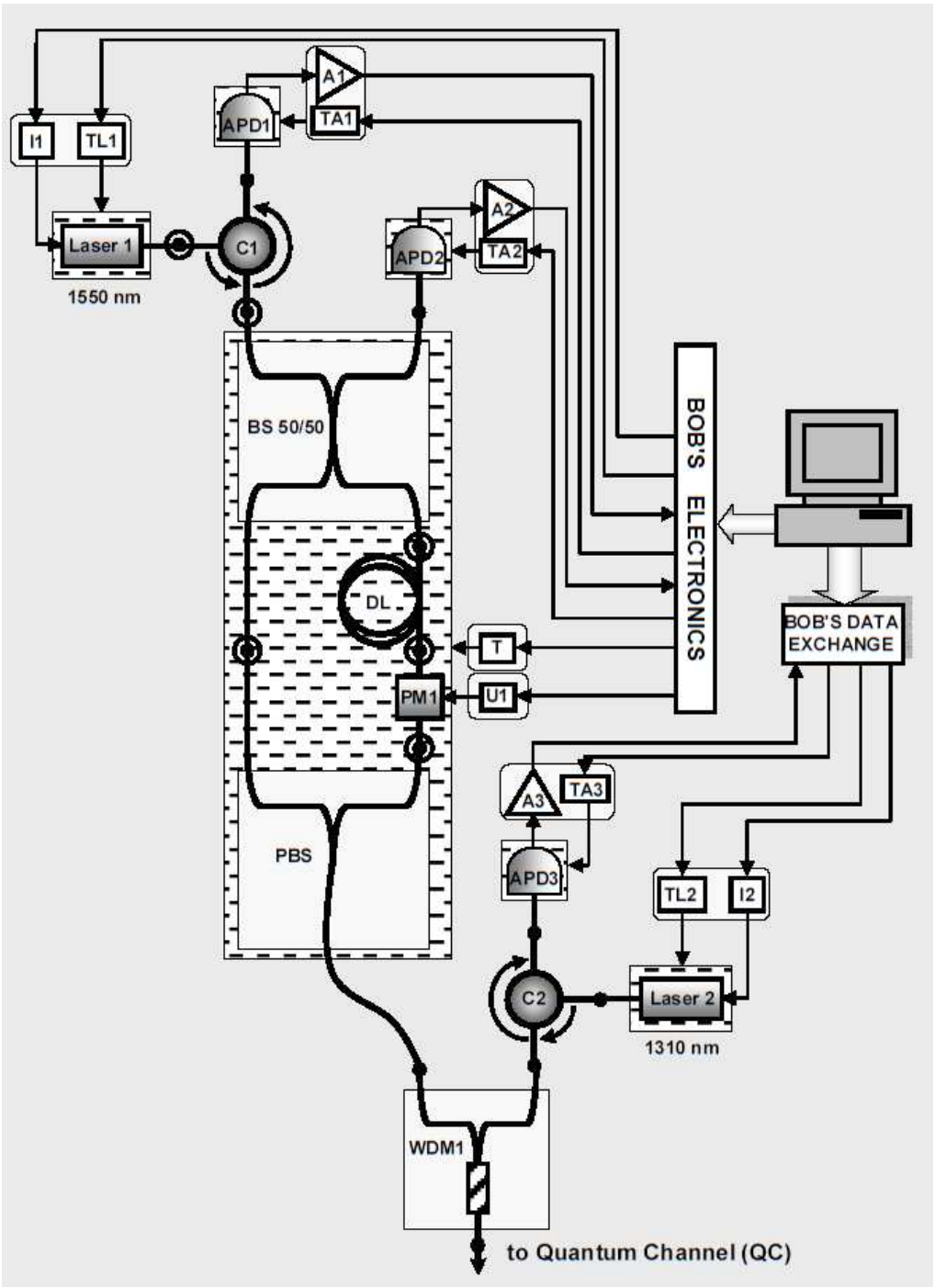

Fig 3.6 Bob part of prototype setup

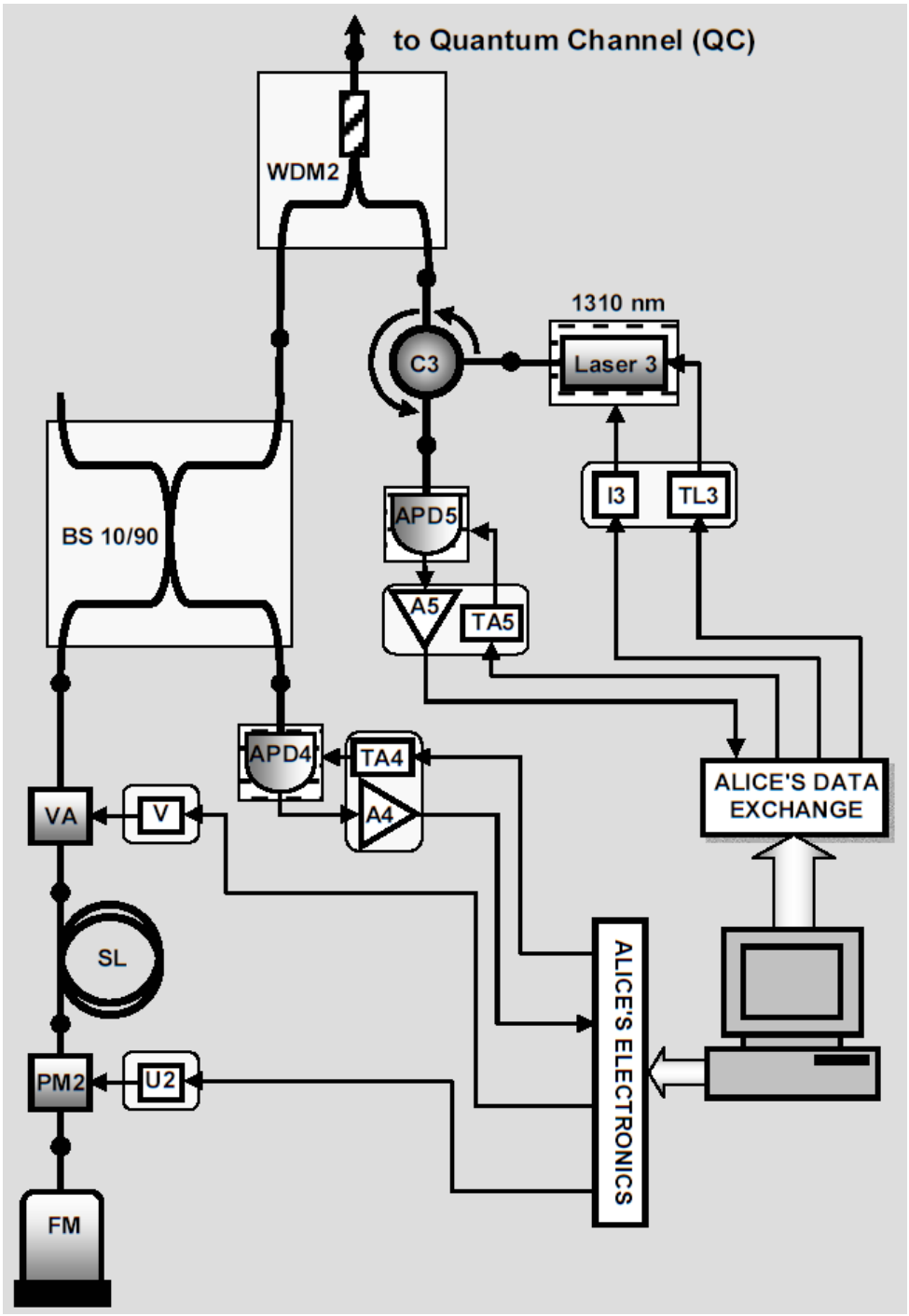

Fig 3.7 Alice part of prototype setup

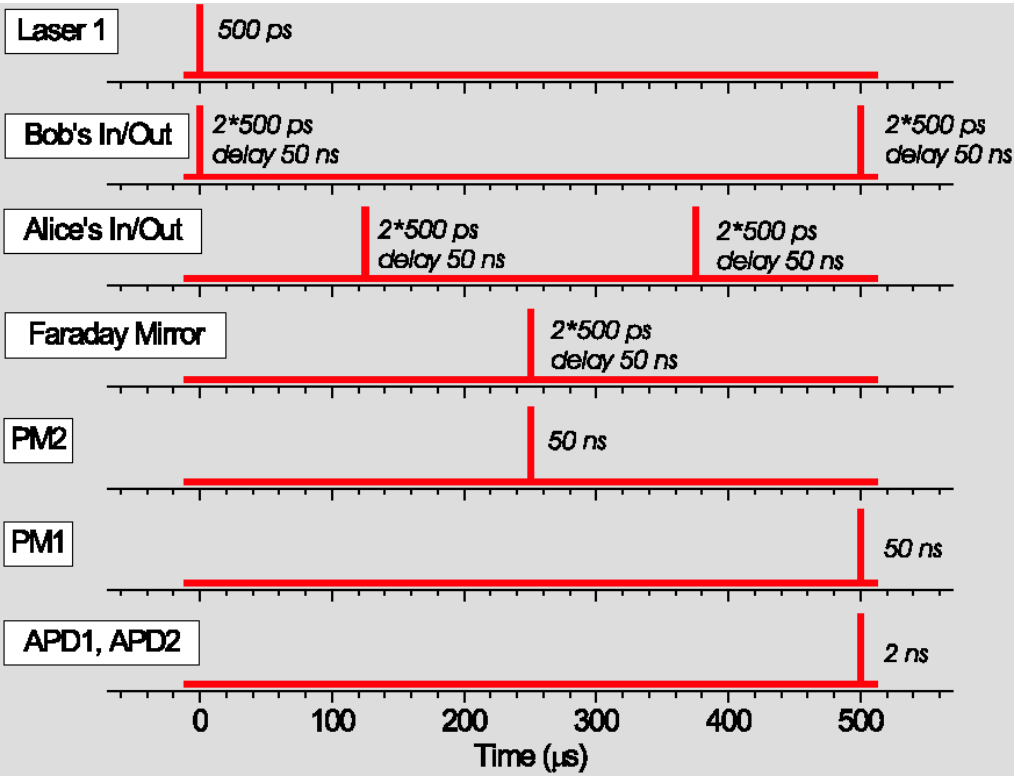

Fig 3.8 Timing Diagram of prototype setup with 25km quantum channel and 25km storage line

Prototype setup의 timing diagram은 Fig 3.8과 같다. Fig 3.8에서 Laser1은 레이저에서 나온 500ps 의 광신호를 나타내며 Bob's In/Out은 Bob에서 출력 입력 광신호의 timing을 나타내는 것으로 50ns의 delay time을 갖는 500ps width를 갖는 펄스 2개가 입출력되는 것을 의미한다. Alice's In/Out에서도 동일하며 25 km QC의 거리만큼 timing 차이가 생긴다. Faraday Mirror에서는 두 광신호가 faraday mirror에서 반사되는 시점을 나타낸다. PM2는 faraday mirror에서 반사된 두 광신호 중 하나에 50ns 펄스 width를 갖는 변조 신호를 인가하는 timing을 나타낸다. PM1은 해당하는 timing에 50ns의 width를 갖는 변조신호를 인가하게 되며 APD1, APD2는 2ns의 width를 갖는 geiger mode 펄스를 인가하는 timing을 의미한다.

3.3.3 Assembly of Optics part

어셈블한 밥과 앨리스의 광학부는 Fig 3.9, Fig 3.10과 같다. 모든 광학 부품은 방열을 위해 2mm 두께의 초두랄루민 위에 고정하였다. 밥의 rotatable FC 커넥터를 제외하고는 모든 광학부에 FC 커넥터를 사용하였다. 이는 편광축 조정을 쉽게 하기 위해서며 광학부품 단위로 광 신호를 측정하여 노이즈를 제거하기 위함이다. 이는 추후 광융착접속기를 이용하여 접속하여 커넥터를 사용하여 생기는 노이즈와 감쇄를 줄여야 한다. 광학부는 알루미늄 케이스로 보호를 하였으며 내부에는 스티로폼 단열재를 이용하여 단열하였다. 그러나 Plug & Play 시스템의 앨리스는 단열을 할 필요가 없으며 밥은 단열이 필요하나 정밀한 온도 제어 시스템은 필요없다. Pahse modulator의 신호 리드선을 가능하면 짧게 하기 위해서 케이스에 가까이 배치하여야 한다.

Fig 3.12는 밥에 있는 간섭계를 이용하여 Fig 3.11과 같은 시스템 구성으로 보강, 상쇄 간섭신호의 비율을 측정했다. 레이저 신호는 continuous mode로 동작하였으며 phase modulator에는 -7~7V 사이의 전압을 인가하였다. 보강, 상쇄 간섭의 비율을 더 높이기 위해서 광신호의 편광축을 rotatable FC 커넥터 세밀하게 조정하여 보정해 주어야 한다.

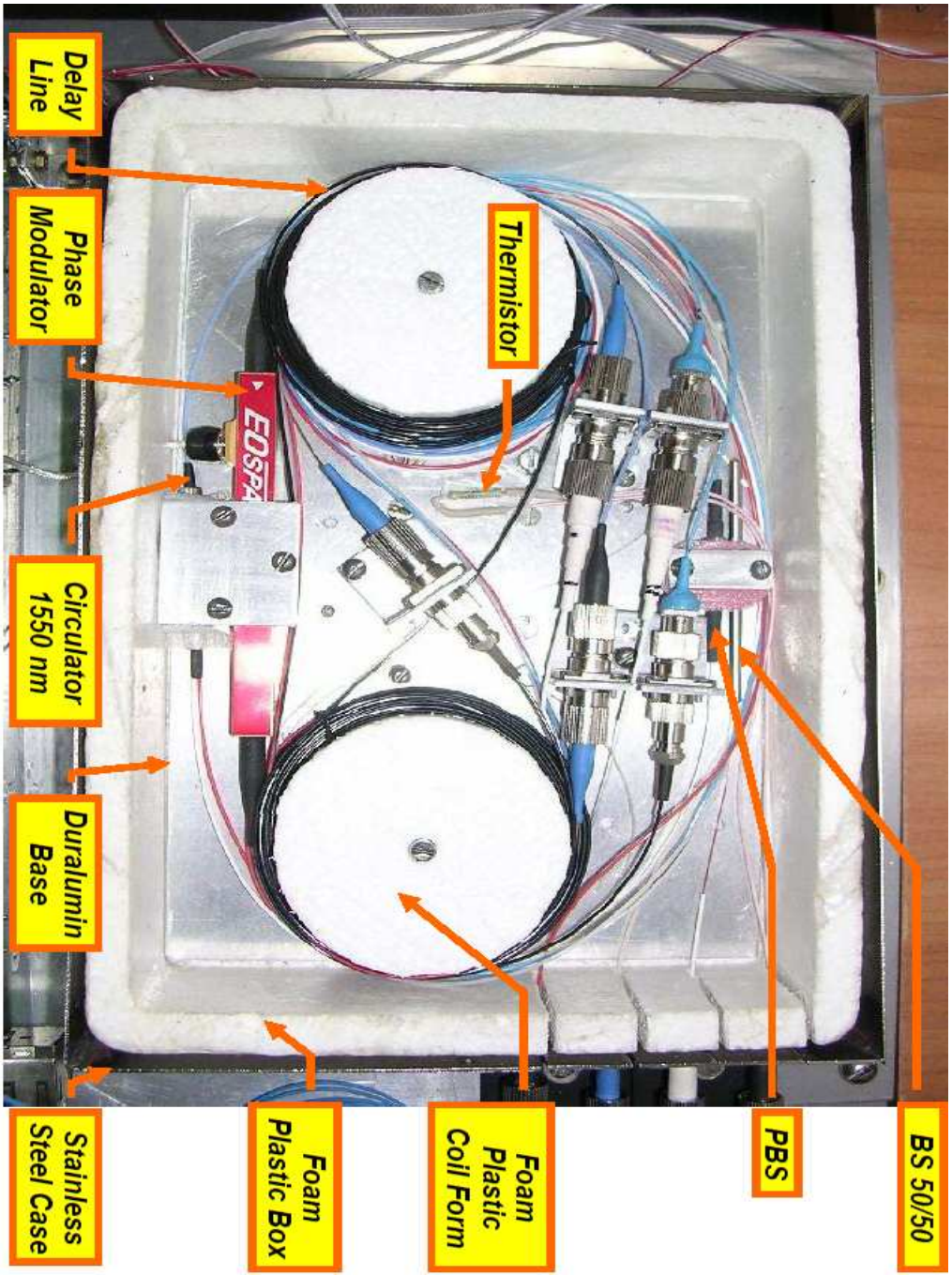

Fig 3.9 The view of BOB Optics

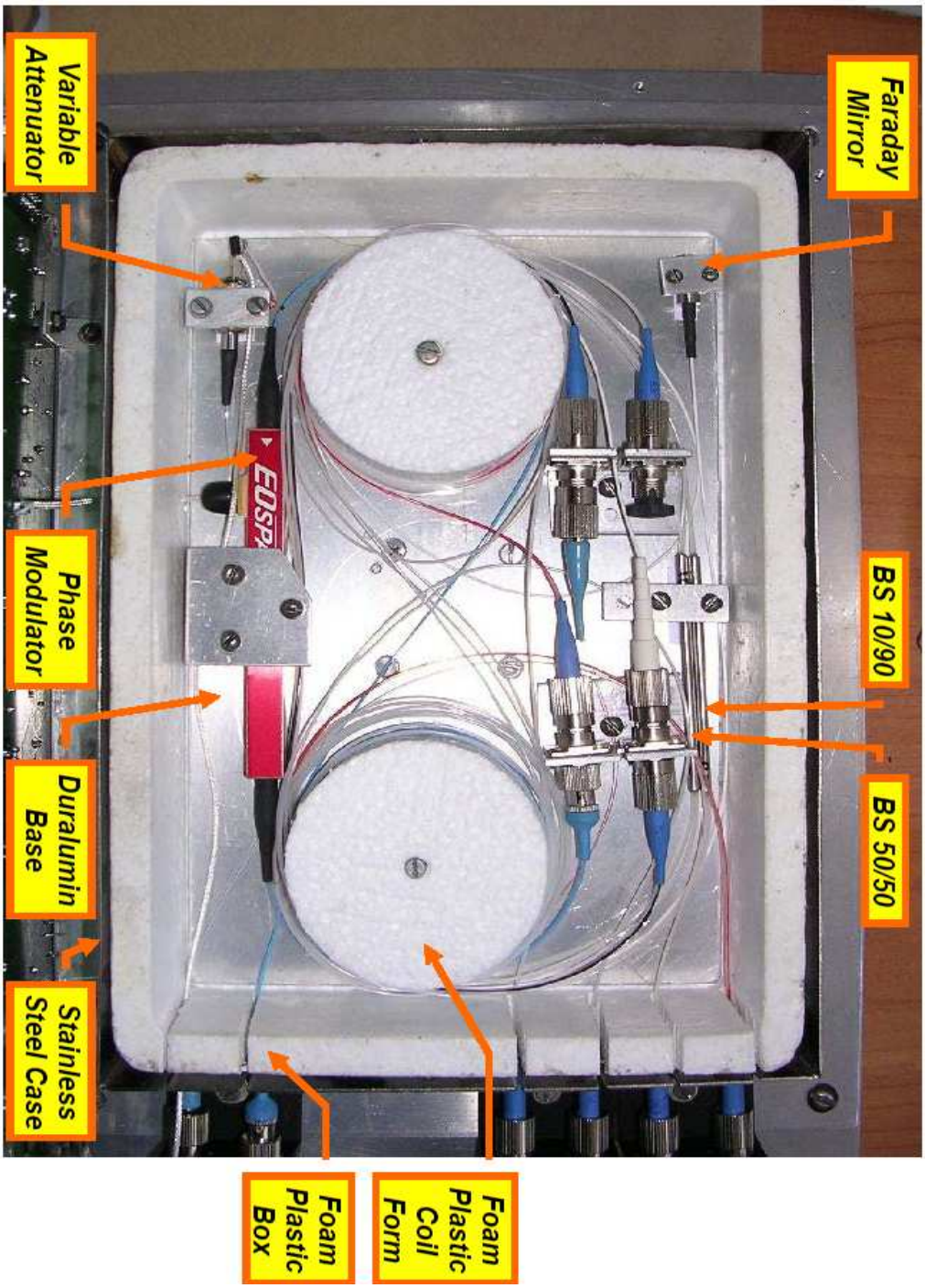

Fig 3.10 The view of ALICE Optics

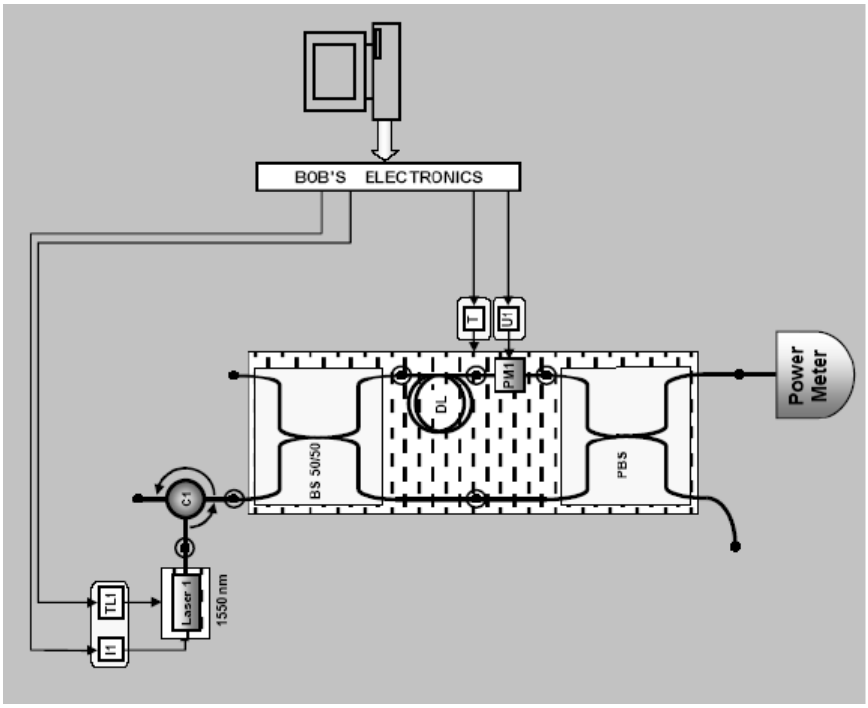

Fig 3.11 Test schemetic of interferometer at BOB in CW regime

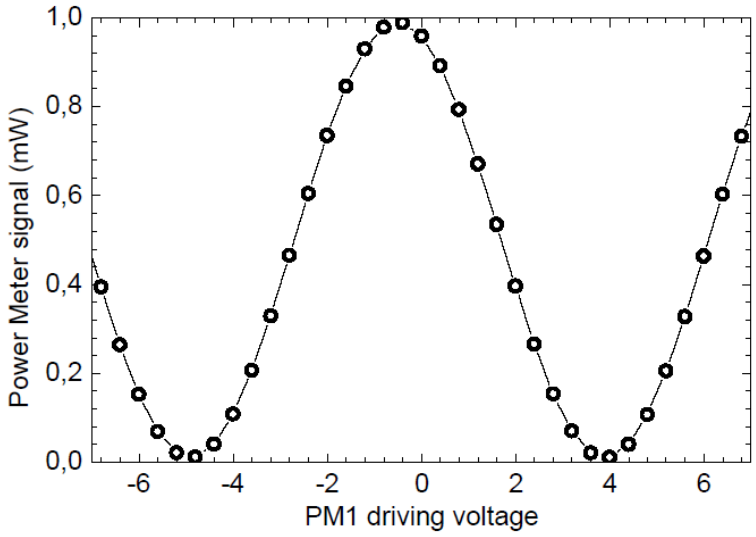

Fig 3.12 Power of output interfered signal in the BOB

3.3.4 Assembly of Electronics part

3.3.4.1 Single-Photon Counting Module

- Amplifier Module

Fig 3.13은 SPCM Block diagram을 나타낸다. 단일광자 검출소자로 InGaAs APD (ETX 40 APD END BA, JDS Uniphase USA)를 사용하였으며 회로 구성은 active quenching circuit을 사용하였다. Dark noise를 줄이기 위해 소자를 -50℃로 냉각하고 Bias Tee와 pulse generator를 이용하여 geiger mode로 동작하였다. Geiger mode 펄스로 2~10ns width와 breakdown 전압보다 2~5V 높은 전압을 갖는 신호를 사용하였다. APD의 출력 신호는 high speed radiofrequency amplifier AMP1을 이용하여 초기 증폭하였으며 이는 또 다른 AMP를 거쳐 analog ouput으로 연결되어 신호를 모니터 할 수 있게 된다. 또한 초기 증폭된 신호는 high speed comparator를 거쳐 단일 광자를 카운트 하기 위한 신호로 증폭이 된다.

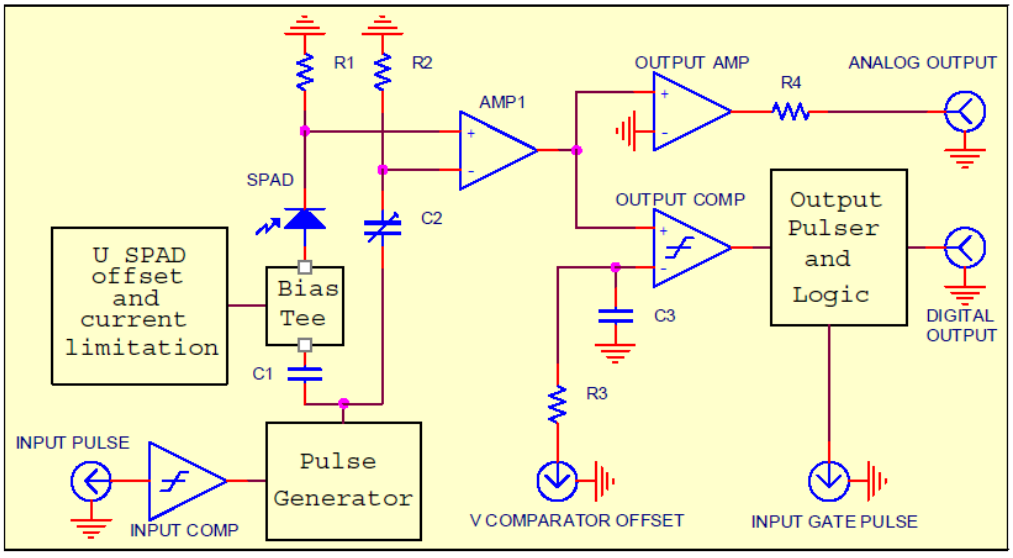

Fig 3.13 Block Diagram of SPCM module

증폭부의 세부 회로 구성은 Fig 3.14과 같다. 기본적으로 three-stage amplifier를 사용하였으며 이의 gain은 controller에 의해 조정되는 digital potentiometer를 이용하여 조정하였다.

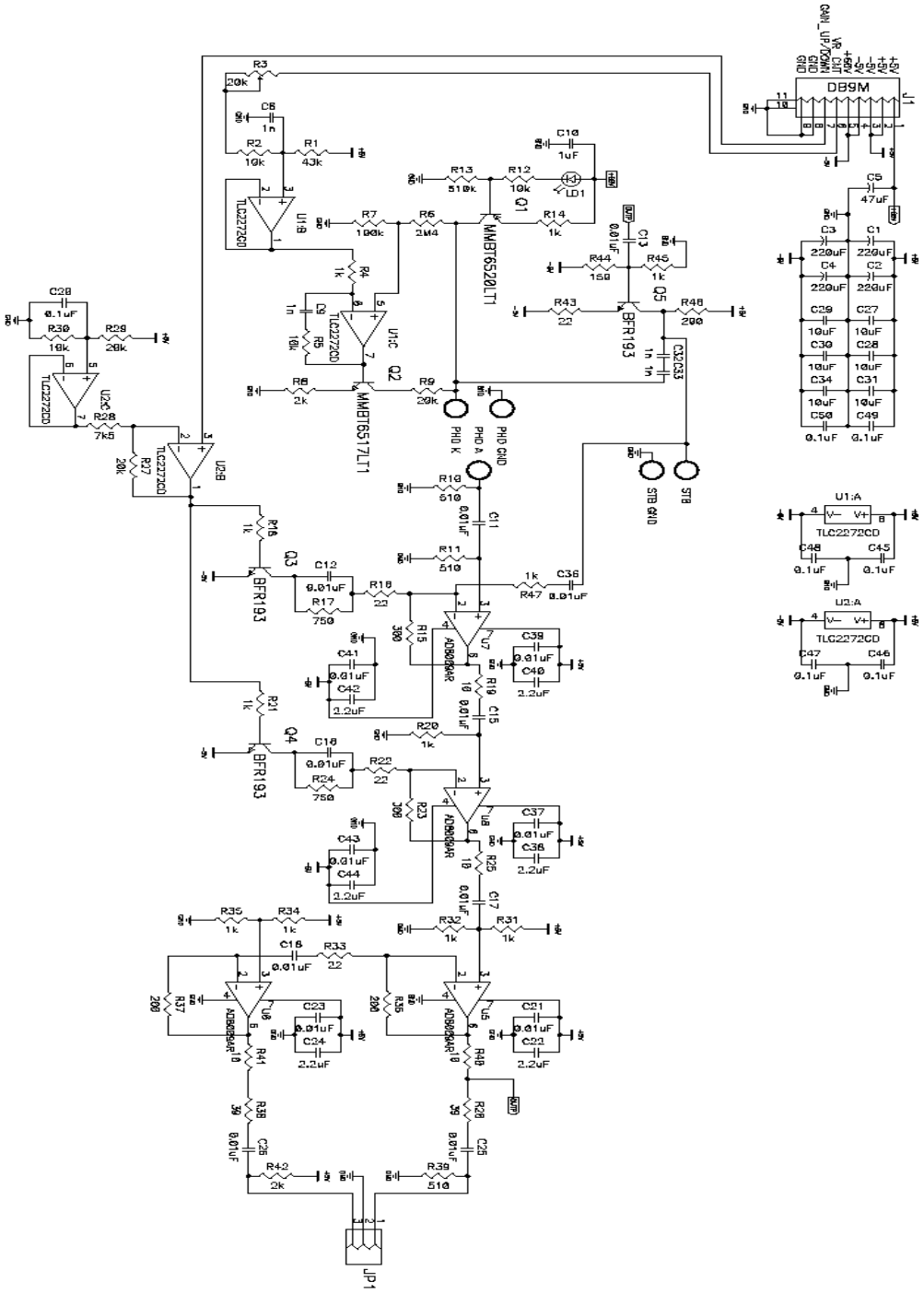

Fig 3.14 Schematic design of Amplifier Module of SPCM

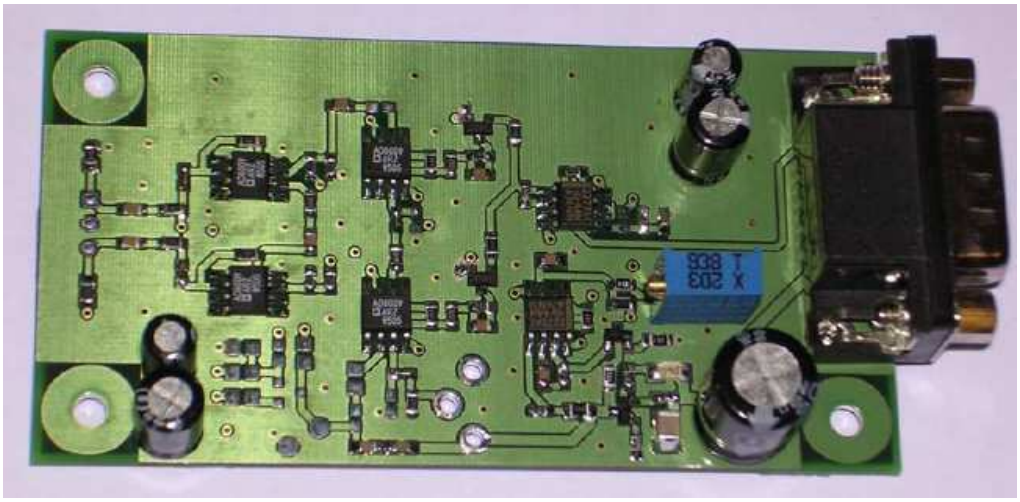

Fig 3.15 View of Amplifier Module of SPCM

-Temperature Controller Module

APD를 냉각하기 위해 열전소자를 사용하는데 이의 controller는 3A 이상의 전류와 10V 이상의 전압을 공급할 수 있어야 한다. Controller는 3개의 OP-Amp를 사용하여 PID control 회로를 구성하였으며 feedback 신호로 HEL-700-U thin film platinum thermoresistor를 사용하였다.

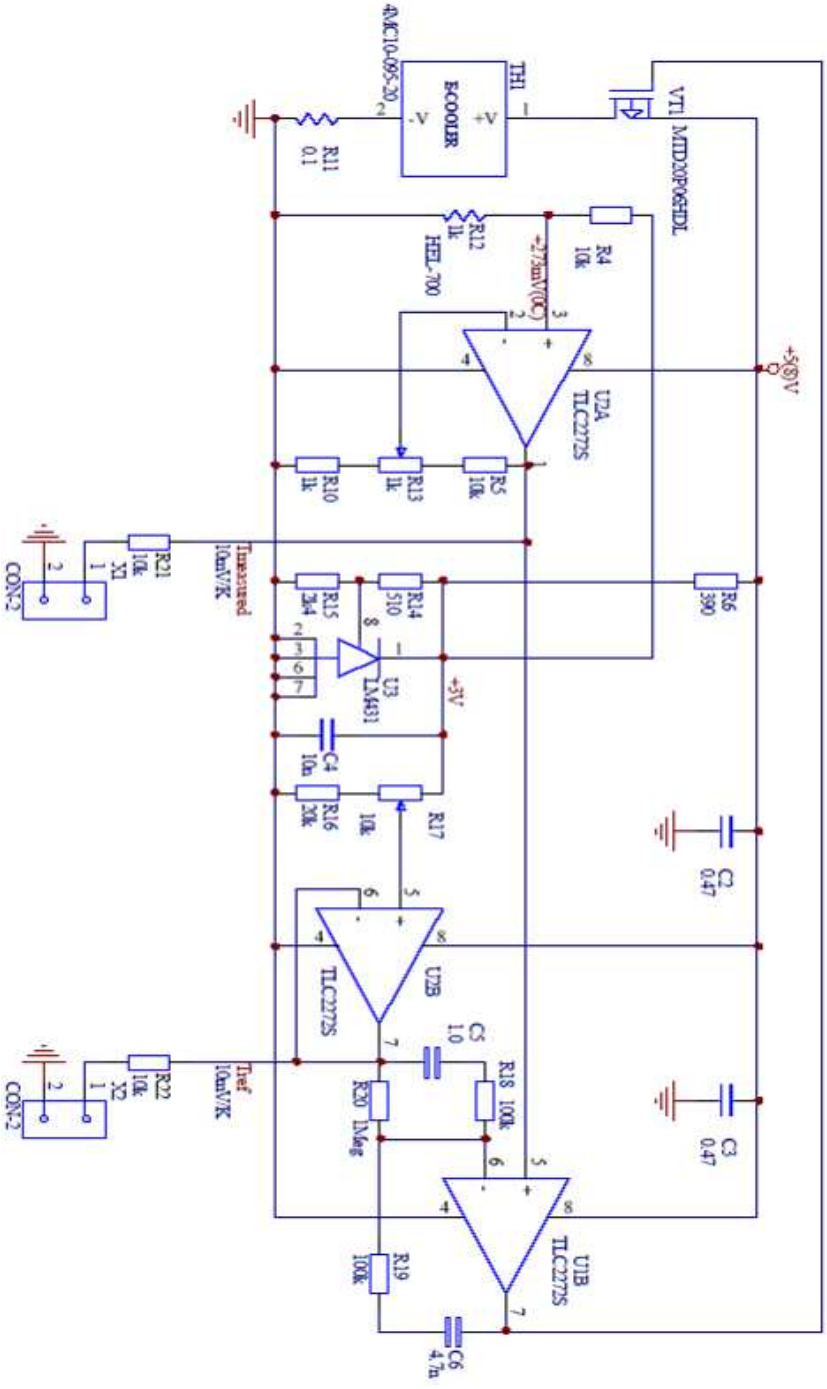

Fig 3.16 Schematic design of Temperature controller module

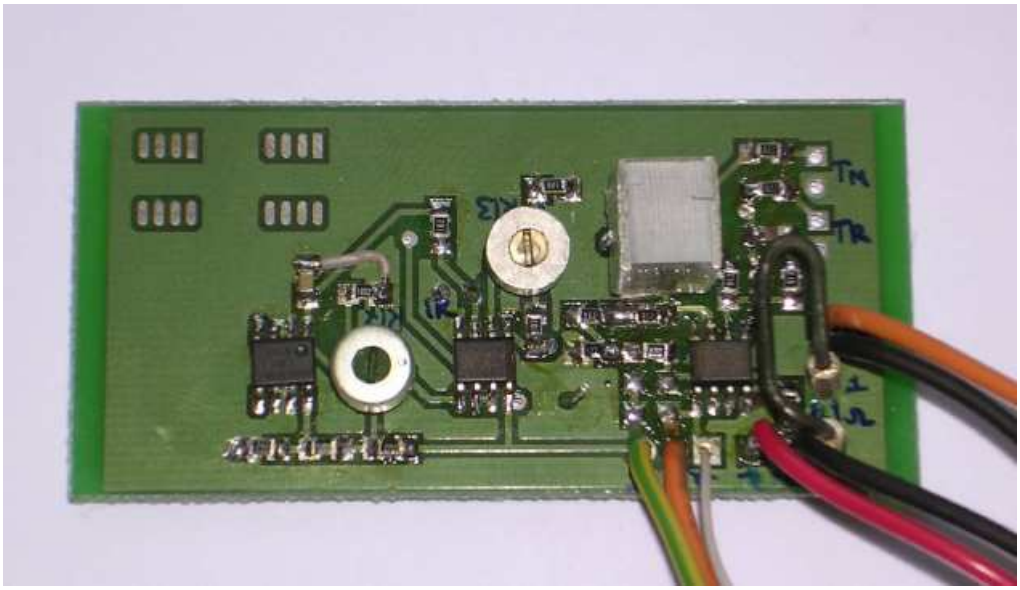

Fig 3.17 View of Temperature controller module

-Power Supply Module

시스템은 2.5V, 3.3V, 5V(logic), 7~15V(TEC), ±15V(analog), 24V, 30~40V(photodiode)의 다양한 전원을 사용한다. 이를 위해 power supply는 2단으로 설계되었으며 1단은 AC-DC, 2단은 DC-DC converter로 구성이 되었다. AC-DC는 220VAC 입력으로 +24VDC 출력전압을 내며 2단에서는 +24VDC를 입력전압으로 사용하여 상기 필요 전원에 맞는 전압을 출력한다. 이의 회로도와 완성된 power supply는 Fig 3.18, 3.19와 같다.

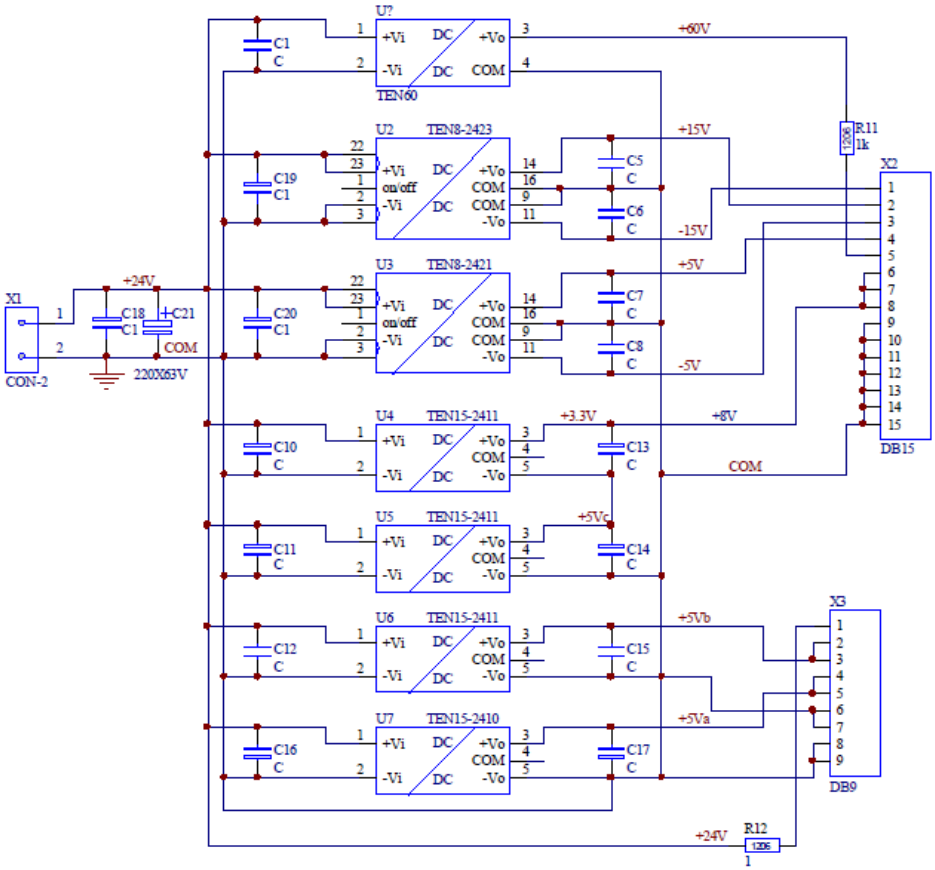

Fig 3.18 Schematic diagram of Power Supply Module

Fig 3.19 View of Power Supply Module

3.3.4.2 Alice & Bob Electronics

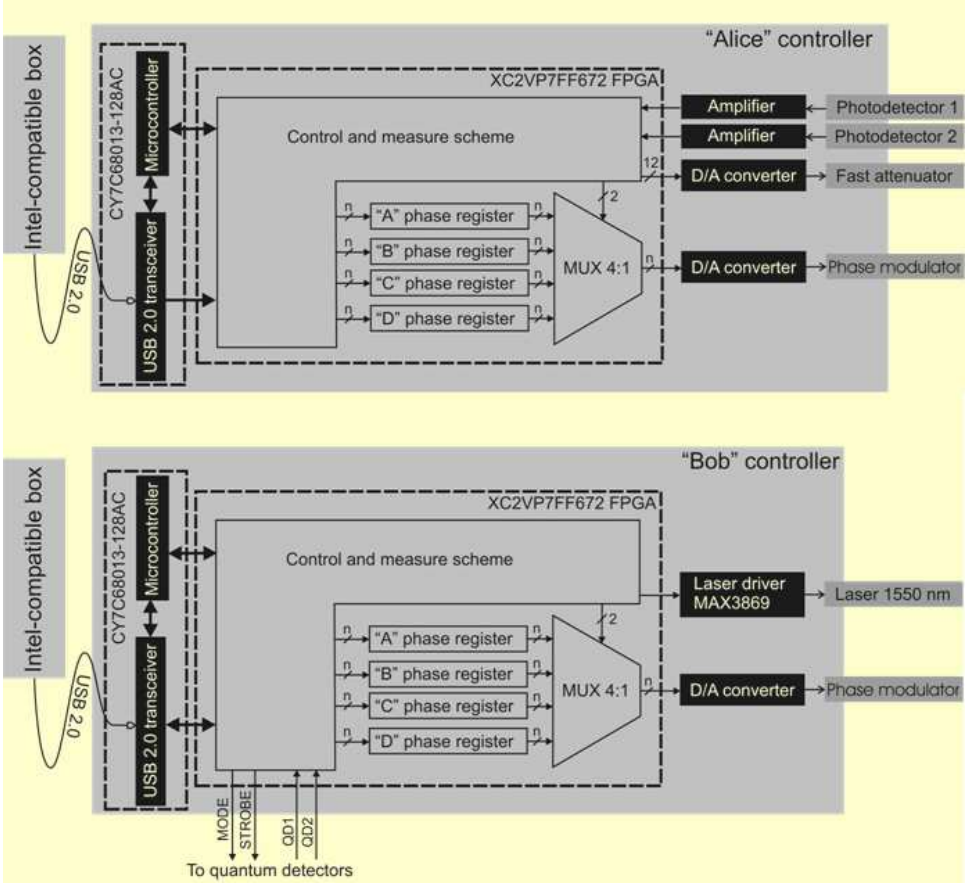

Fig 3.20 Block diagram of controllers of Alice and Bob

Fig 3.20 은 앨리스와 밥에 설치된 controller board의 기능에 따른 block diagram을 나타낸 것이다. 양자암호 키 분배를 위한 shell 프로그램을 통해 양자암호 키 분배를 위한 조건을 컴퓨터를 통해 지정해주며 이러한 명령어들은 USB 인터페이스를 갖춘 USB MCU(Cypress MicroController Unit CY7C68013-128AC)로 전달이 된다. USB MCU는 신호 제어를 위한 FPGA Chip과 연동되어 있다. FPGA는 Timing control, laser driver, phase modulator 값을 생성하는 기능 등의 양자암호 키 분배의 제어와 관련된 대부분의 기능을 수행하게 된다. 중요 기능과 관련된 회로도를 도시하였으며 이를 7-Layer로 구성된 다층 PCB로 제작하였다. 이는 Fig 3.21부터 Fig 3.28에 나타내었다. Fig 3.29와 Fig 3.30은 Controller board와 Driving board를 시스템에 setup한 사진이다.

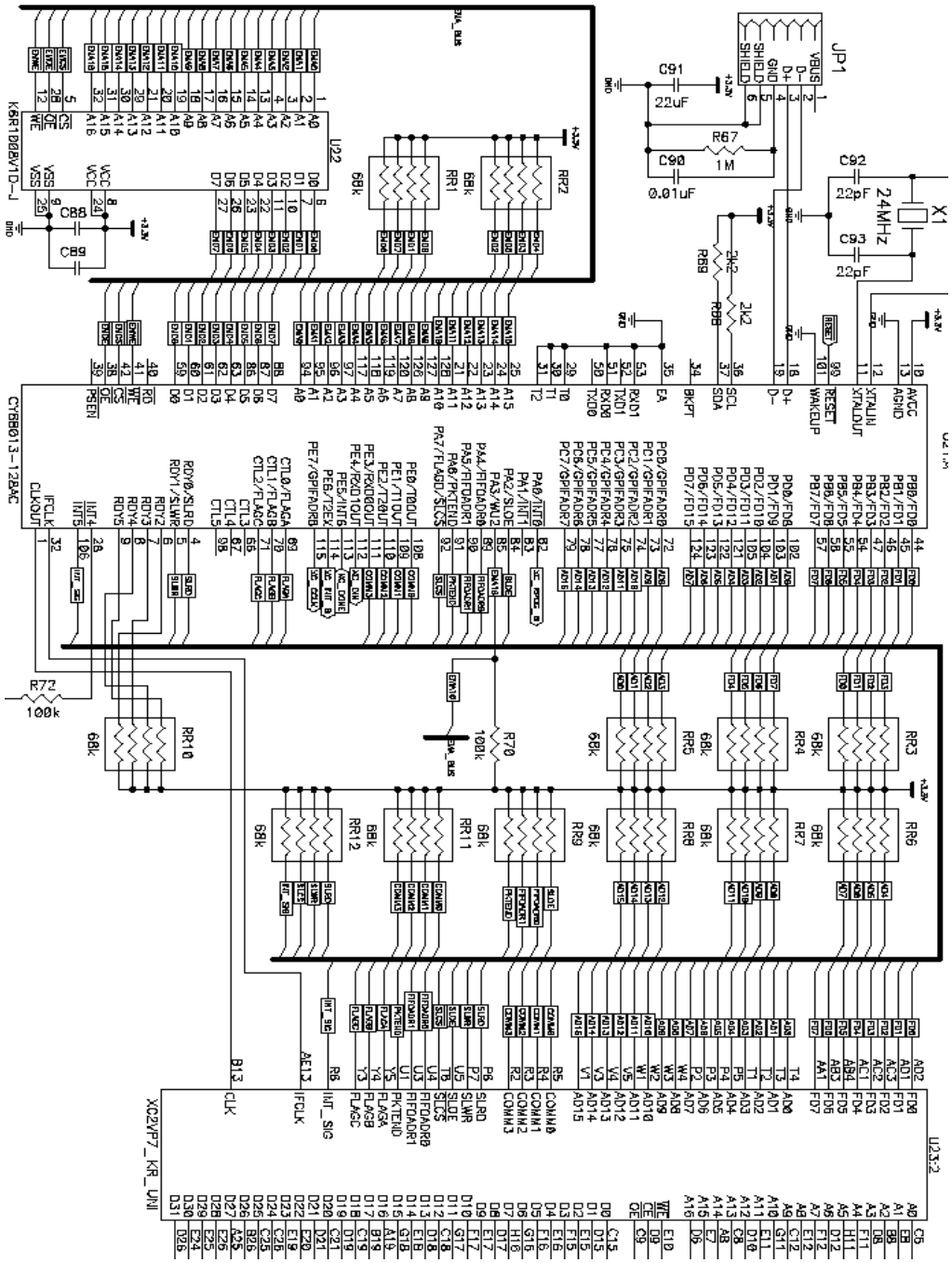

Fig 3.21 Schematic design of the CPU unit of Controller PCB of Alice and Bob

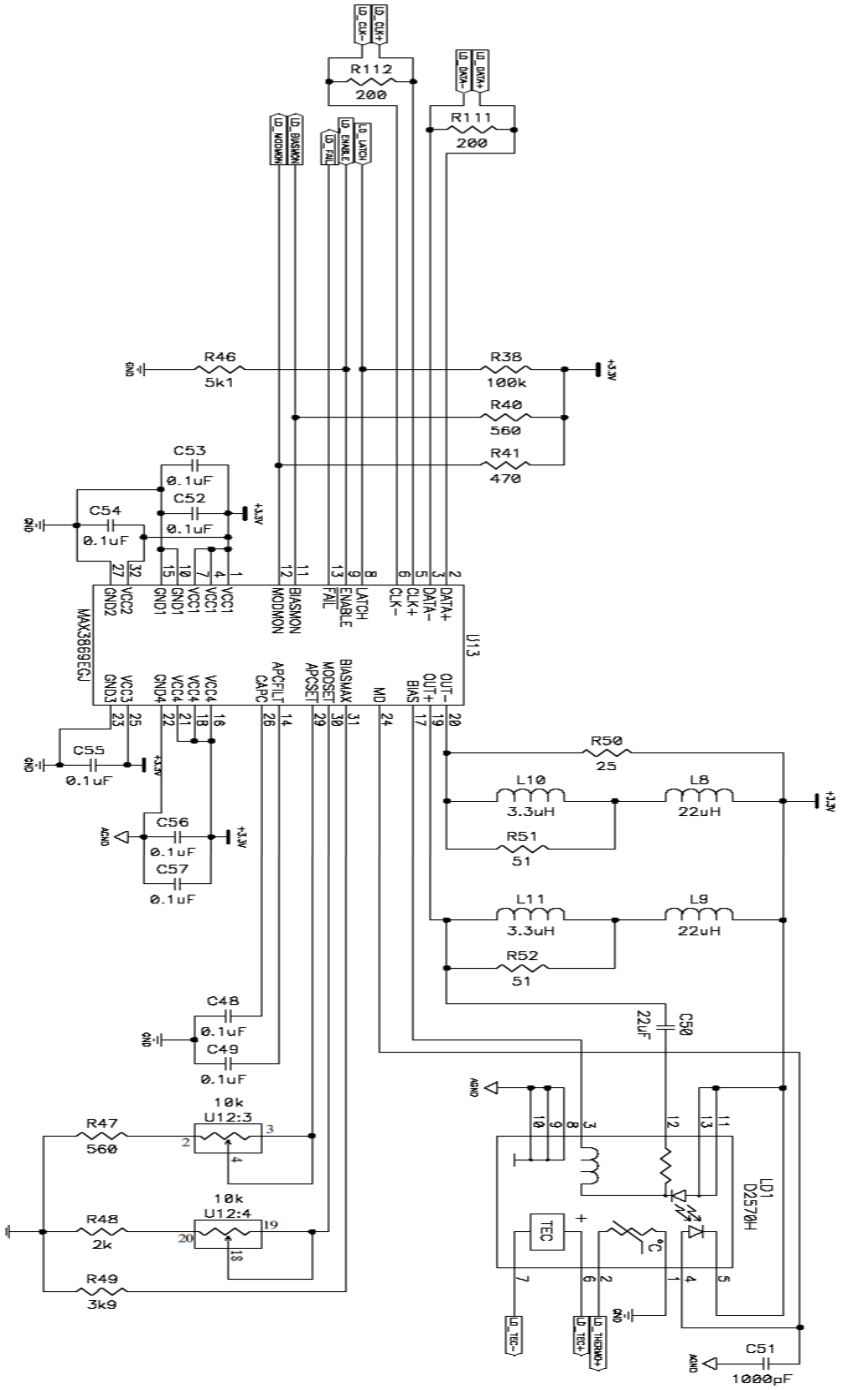

Fig 3.22 Schematic design of the laser Diode driver

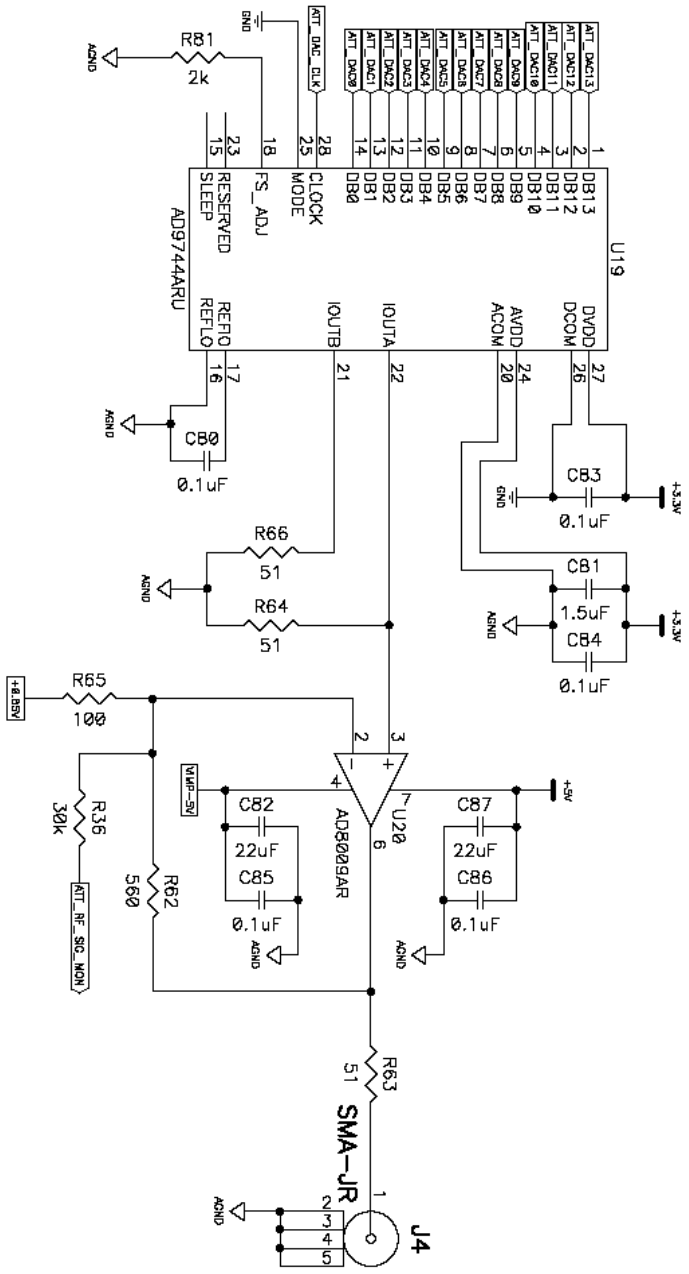

Fig 3.23 Schematic design of the phasemodulator, variable attenuator

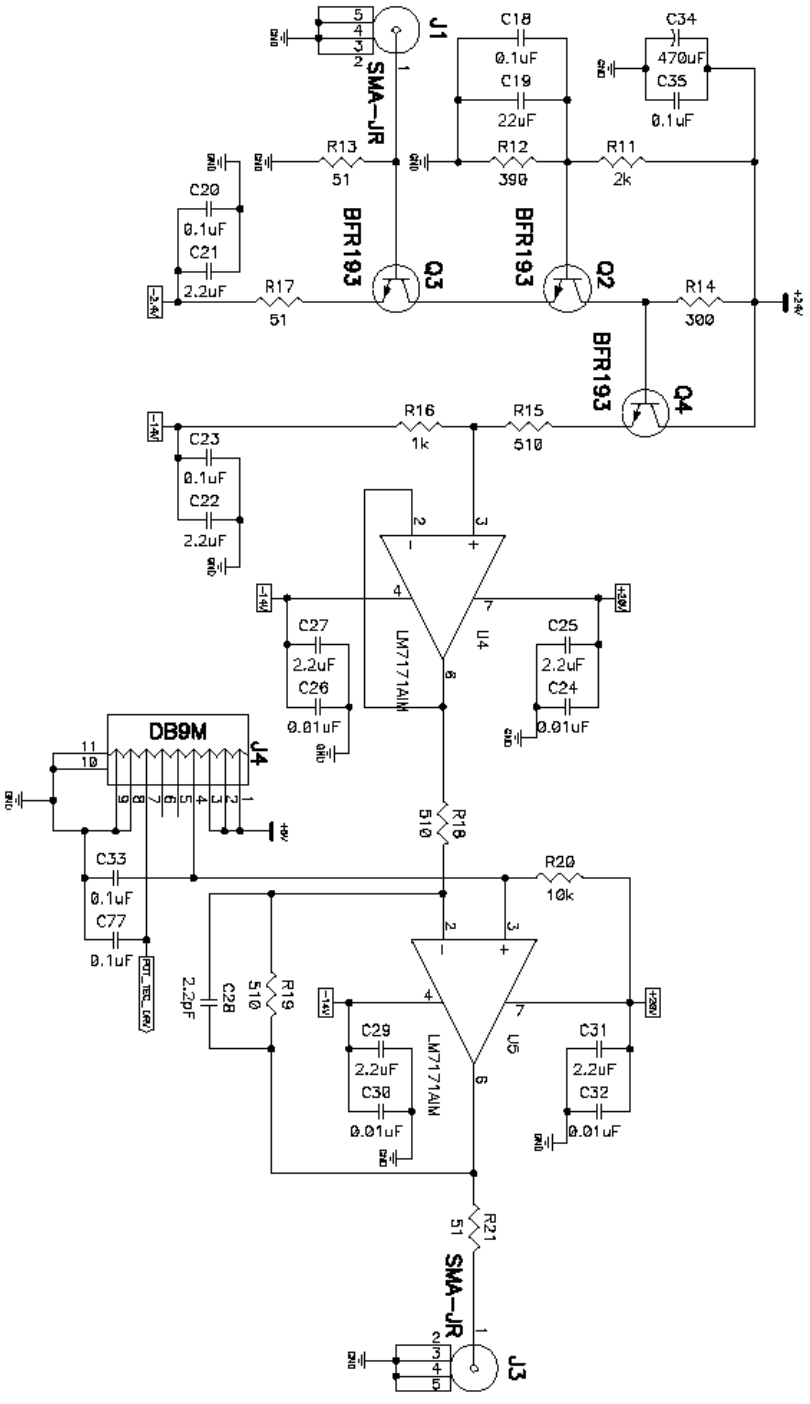

Fig 3.24 Schematic design of the driving amplifier

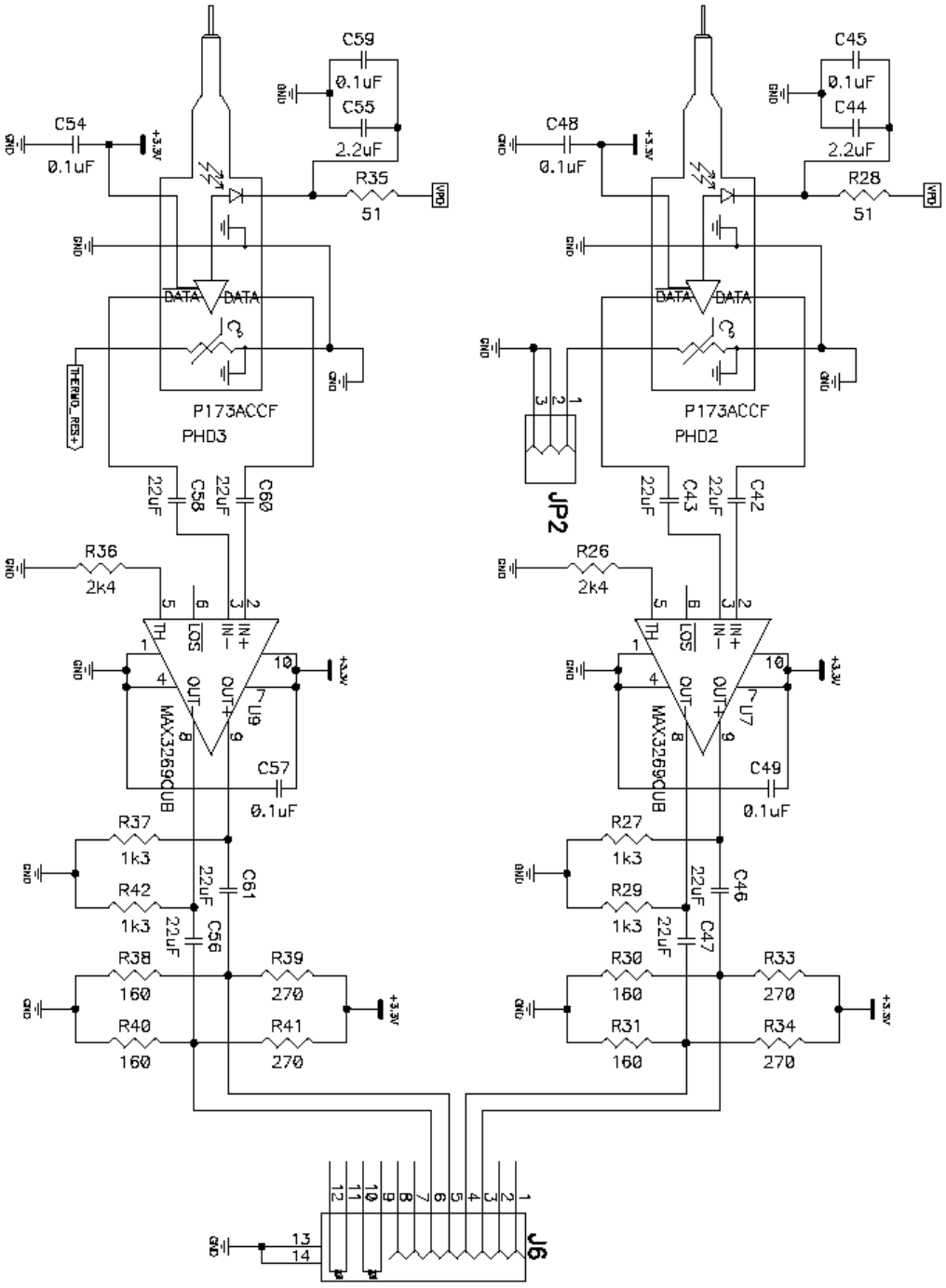

Fig 3.25 Schematic design of the monitor PD

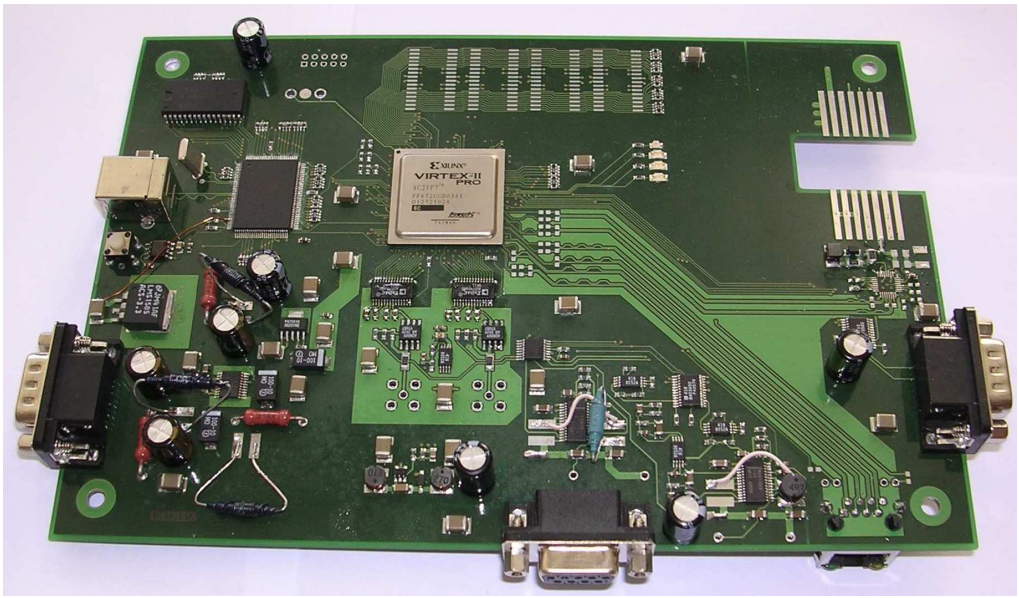

Fig 3.26 View of the Controller PCB of Alice

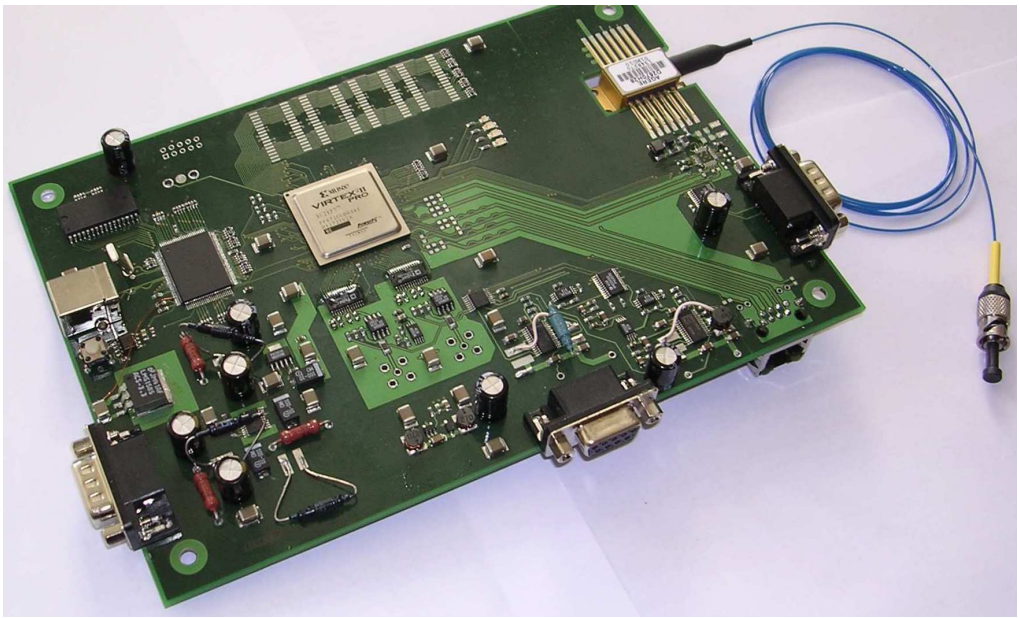

Fig 3.27 View of the Controller PCB of BOB

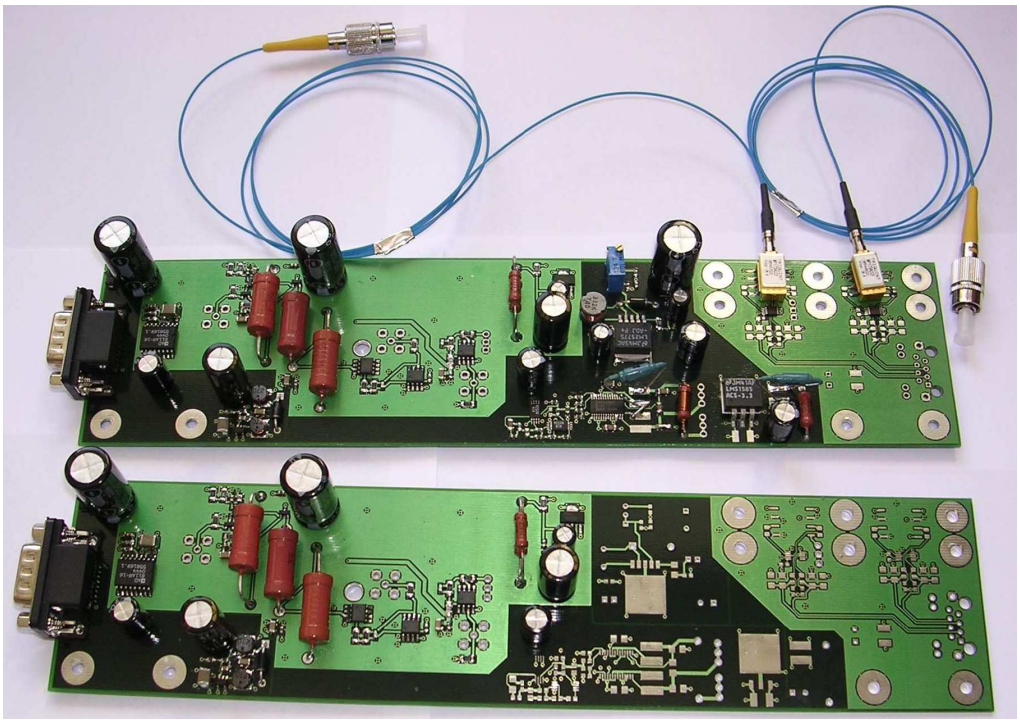

Fig 3.28 Driving PCB of Alice and Bob

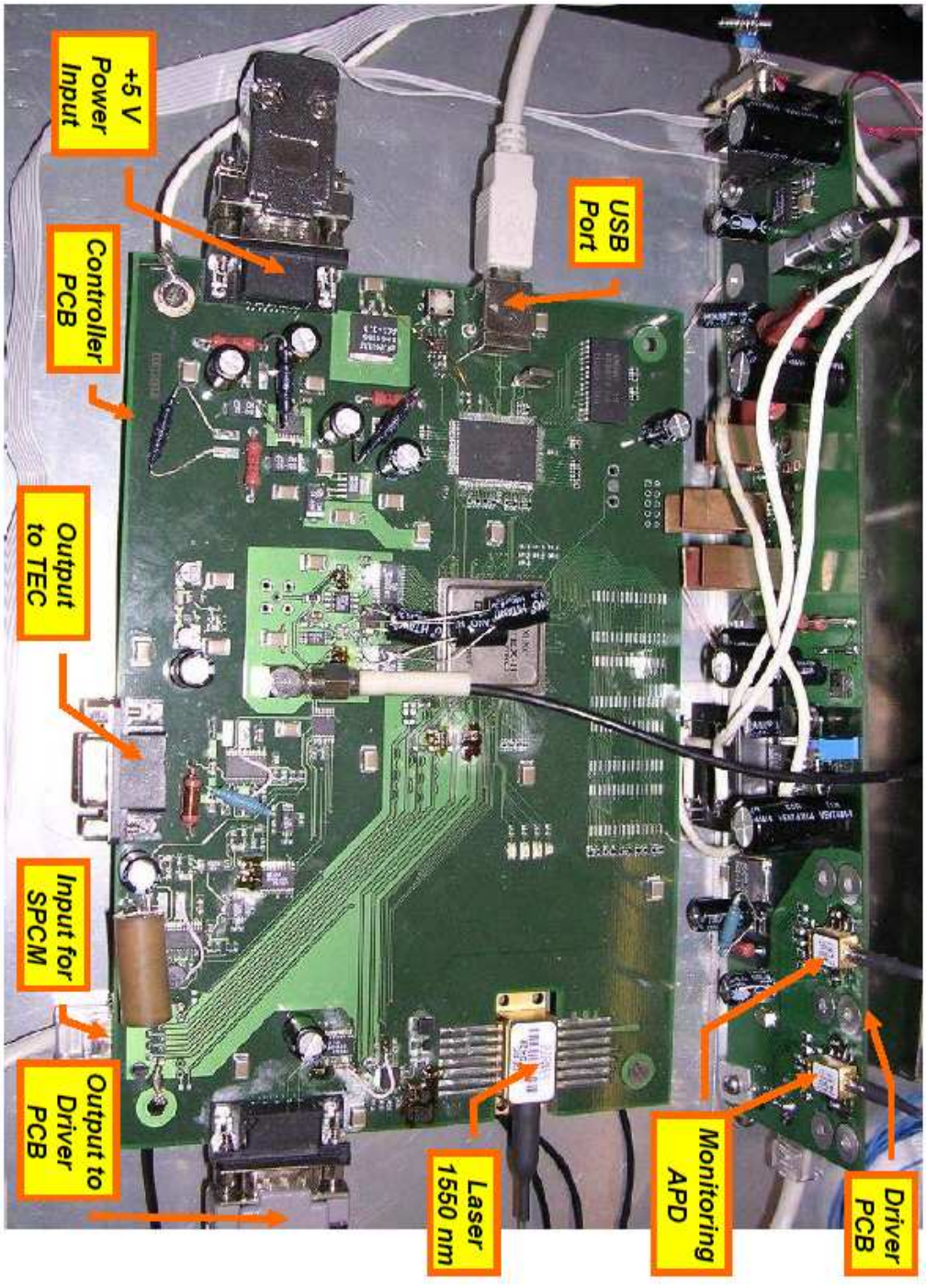

Fig 3.29 The view of BOB assembled electronics

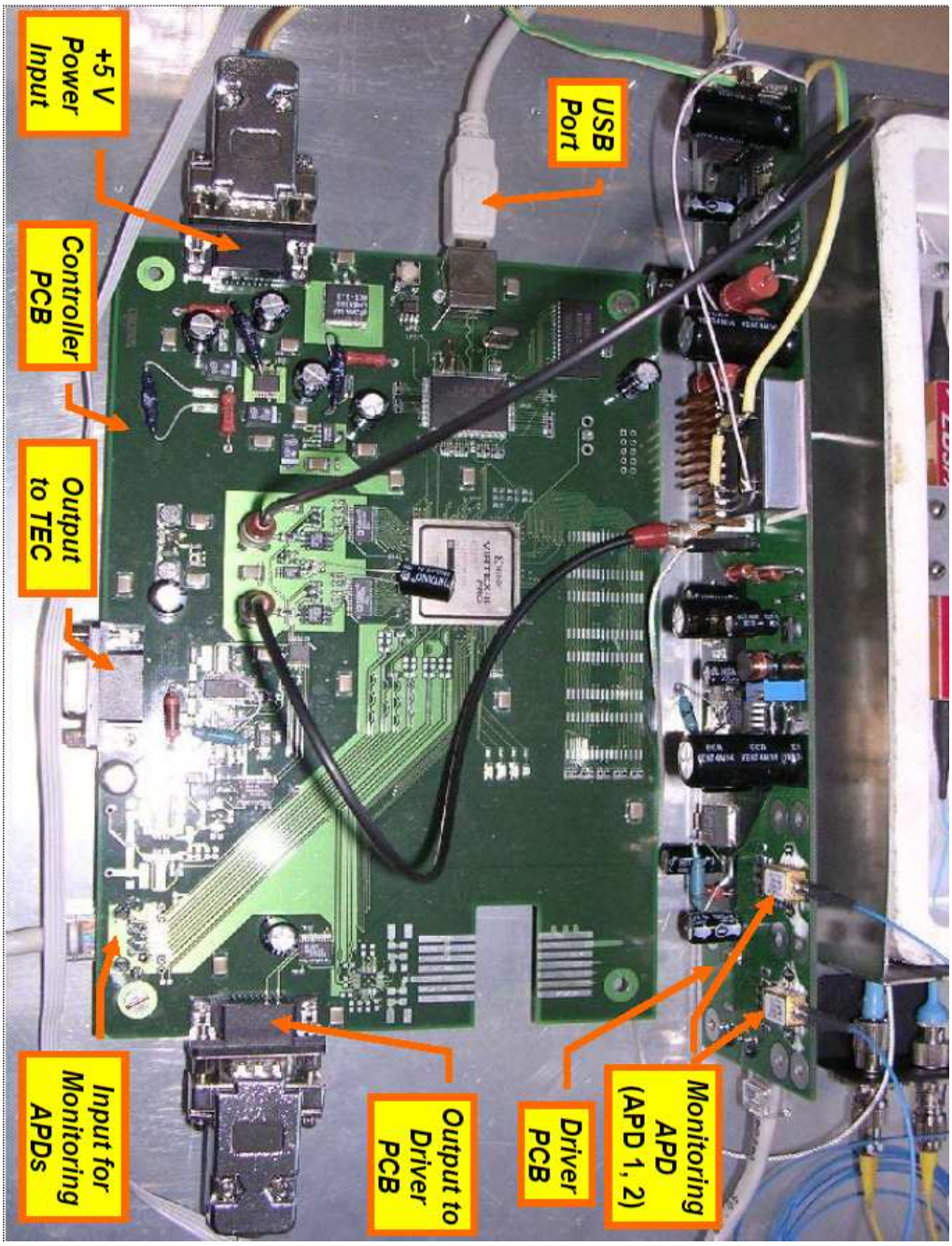

Fig 3.30 The view of ALICE assembled electronics

3.3.5 Experiment Results of Plug & Play QC System

구현된 Plug & Play system 상에서 25km 양자채널(광섬유)과 이더넷 네트워크를 이용한 공개채널을 사용하여 양자암호키 분배 실험을 하였다. 양자암호키 분배 parameter와 관련한 자세한 설명은 5.2절에 기술하였다. 실험 순서는 다음과 같다.

Alice와 Bob의 모든 제어는 컴퓨터를 이용하여 작동하였으며 multi-photon laser pulse를 이용하여 time delay, phase modulator의 phase, variable attenuator의 attenuation을 미리 최적화 한다. 그리고 난후 시스템을 양자키 분배 모드로 전환하여 유사 단일 광자를 생성 및 전송을 하게 된다. laser는 25.6 kHz의 주기를 갖는 pulse train으로 동작이 되며 이와 동시에 Bob에 있는 SPCM의 reverse bias를 조정하여 양자효율 15%, Dark Noise $8x10^{-5}$ count/gate를 유지하게 된다. SPCM에서 검출된 신호는 메모리에 저장되어 양자키 분배 모드가 종료되면 컴퓨터로 읽어지게 되어 Alice와 Bob사이에 공개채널을 통하여 phase modulation 값을 서로 공유하게 된다. 결국 BB84 protocol에 따라서 sift key를 생성하게 된다.

Table 3.2는 sift key rate와 error rate에 대해서 이론값과 실험값을 나타낸다. 실험조건은 양자채널 25km, 채널 감쇄율 T=0.1, laser driving frequency f_L=5MHz, laser pulse frequency f_{eff}=25.6kHz, Dark Count Probability $P_D=8\times10^{-5}$ count/gate, 양자효율 η=15%, 평균 광자수 μ=0.2 photons, visibility V=0.985 를 적용하였다. 이론값은 실험 조건을 고려하여 5.2절의 식 5.2~4를 이용하여 나타내었다. sift key rate는 이론값과 실험값이 비슷하며 error data는 실험값이 더 좋게 측정되었다. 이는 더 작은 width의 gated geiger mode pulse를 사용했기 때문이다. 측정된 sift key rate 속도는 35 bps를 기록하였으나 이는 pulse train의 속도를 조정하여 향상시킬수 있다. 그러나 구현된 시스템에서는 USB driver program의 문제로 인해 pulse train의 속도를 30kHz 이상 구현 할 수 없다.

	Experiment	Theory
R_{sift} (bit/s)	35±3	38.4
R_{err} (bit/s)	0.8±0.1	1.31
Q_{BER} (%)	2.3±0.3	3.3

Table 3.2 양자암호키 분배 실험 결과

제 4 장 위상안정화 광섬유를 이용한 단일방향 양자암호시스템 구성

Plug & Play 시스템은 광섬유 상에서 전송시 위상변화가 생기는 문제점을 왕복구조를 이용하여 해결하였다. 그러나 backscattering에 의해 제한 받는 전송 속도, 전송 거리와 단일광원을 사용하기 어렵다는 점은 큰 단점으로 작용한다. 또한 네트워크 적용에도 어려움이 있으며 광부품 소자들을 많이 사용하는 것 또한 단점으로 볼 수 있다. 이러한 대안으로 본 논문에서는 위상안정화 광섬유를 이용한 단일방향 양자암호 시스템을 제안한다. 단일 방향 양자암호 시스템은 3.2 절에서 설명하였듯이, 비대칭 Mach-Zehnder 간섭계를 연결하여 구성한 것이다. 단일 구조의 장점은 전송 속도와 거리를 증가 시킬 수 있으며 단일 광원 적용도 가능하다. 또한 네트워크 적용이 비교적 쉬운 시스템이다. 그러나 온도, 물리적 변화로 생기는 위상 변화는 단일 방향 시스템 구성에 어려움으로 작용했었다. 지금껏 여러 연구진은 이를 ±0.01℃ 수준의 정밀한 온도보정 시스템을 이용하여 위상 안정을 유지하였으나 제안된 시스템은 위상안정 광섬유를 이용하여 온도 보상 없이 단일방향 구조에서 위상 안정을 구현하였다.

제 4.1 절 위상안정화 광섬유

일반 광섬유의 클래딩은 SiO_2, 코어는 SiO_2 외에 GeO_2가 첨가된 유리 성분으로 코어의 굴절률이 클래딩보다 높아 광신호가 코어를 따라 도파하게 된다. 또한 광섬유의 재료는 석영 유리계 성분이지만 온도에 따라 열팽창이 발생한다. 이러한 이유로 광섬유를 이용한 간섭계는 온도 변화 따라 열팽창 정도가 달라지면서 간섭의 안정성에 영향을 주게 된다.

위상안정화 광섬유는 코어 성분으로 SiO_2와 GeO_2 외에 B_2O_3 유리 성분을 함유

시켜 열팽창 계수를 0으로 조절하게 되며 B_2O_3 2-10 Mol%로 성분비를 조절한다. 또한 코어와 클래딩 사이에 내부 클래딩을 두어 단일 모드 조건을 유지하게 되는데 이는 F와 P를 첨가하여 조절한다. Fig 4.1은 B_2O_3와 F를 첨가하여 0에 가까운 열팽창계수와 단일모드 조건을 가진 광섬유의 굴절률 분포를 나타낸다.

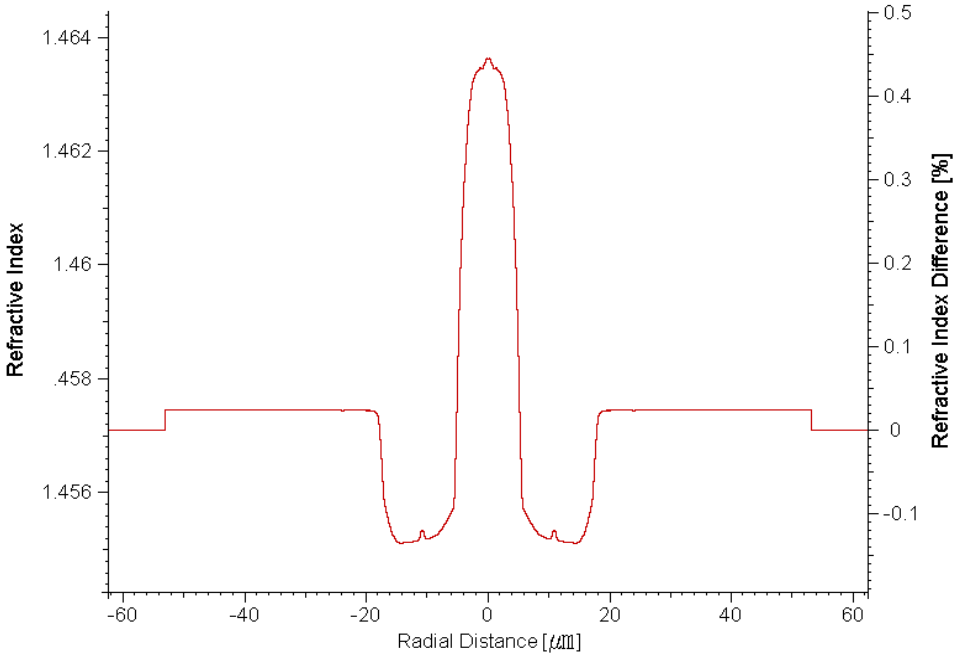

Fig 4.1 위상안정화 광섬유의 굴절률 (B_2O_3/F 첨가)

제 4.2 절 시스템 구성

단일방향 양자암호 시스템의 구성은 Fig 4.2와 같다. 전체적으로 비대칭의 Mach-Zehender 간섭계로 이루어지며 앨리스는 DFB laser diode (JDS Uniphase, ETX 40 APD END BA)와 3dB beamsplitter, 12.5-GHz low-noise E/O phase modulator (EOSpace, PM-0K1-12-PFU-PFU-UL), 1m length의 delay line (단일모드 위상안정화 광섬유), 단일광자 생성을 위한 passive attenuator로 구성 된다. 밥은 앨리스와 마찬가지로 3dB beamsplitter, 1m length의 delay line, 12.5-GHz low-noise E/O phase modulator, Avalanche photodiode (NEC NR8300FP-CC)와 amplifier로 이루어진 single photon counter module, frequency counter로 구성이 된다. SPCM은 다음 절에서 자세히 다루겠다. 앨리스와 밥 사이에는 단일광자 전송을 위한 단일모드 광섬유가 있게 된다.

온도 변화에 따른 위상 변이를 제거하기 위해서는 위상안정화 광섬유를 앨리스와 밥의 long path와 short path에 동일한 길이로 적용한다. 이는 광융착접속기를 이용하여 접속하였다. 단일모드 광섬유와 위상안정화 광섬유를 서로 융착시킬 때는 단일모드 광섬유의 길이와 long, short path의 길이를 최소화 해야 한다. 단일모드 광섬유 길이가 증가 되면 열팽창 계수가 증가 하게 되며, long path와 short path의 길이가 증가하게 되면 마찬가지로 열팽창 정도가 광섬유 체적에 비례하여 증가하게 된다. Fig 4.2에서는 광융착 접속을 위해 단일모드 광섬유로 약 15cm 정도가 포함되어 있으며 phase modulator의 pigtail 편광유지 광섬유로 약 2m 가량이 포함되어 있다. long path는 단일모드 광섬유, 편광유지 광섬유, delay line을 포함하여 약 3m 길이가 되며, short path는 약 1m 길이가 된다. 밥의 광섬유 길이도 앨리스와 같아야 한다. 추후 path length를 줄이고 phase modulator의 pigtail 편광유지 광섬유도 위상안정화 광섬유로 대치하게 된다면 향상된 안정성을 보일 것이다.

시스템 구성시에는 광신호의 편광을 고려해야 한다. phase modulator의 입력포트의 편광축과 short path의 위상안정화 광섬유의 편광축은 같아야 한다. 이는

커넥터를 이용하여 해결할 수 있으나 커넥터를 이용하게 되면 미량이지만 광감쇄가 발생하고 길이를 맞추기 힘들다는 단점이 생긴다. 편광축이 다르게 된다면 간섭된 광신호의 최대값이 다르게 나오게 된다. 앨리스와 밥의 편광축을 같게 만들게 되면 quatnum channel 상에서 발생하는 편광 변이는 밥의 beamsplitter 앞단에 polarization controller를 이용하여 조절할 수 있다. 제작된 위상안정화 광섬유는 비교적 높은 2 dB/m의 광감쇄율을 가지고 있으며 polarization controller를 사용하게 되면 광감쇄율이 상당히 높아지게 된다. 앞에서 말했듯이 이를 해결하기 위해 회전 가능한 커넥터를 사용해야 한다. 그러나 Fig 4.2의 시스템은 커넥터를 쓰지 않고 제작하였다.

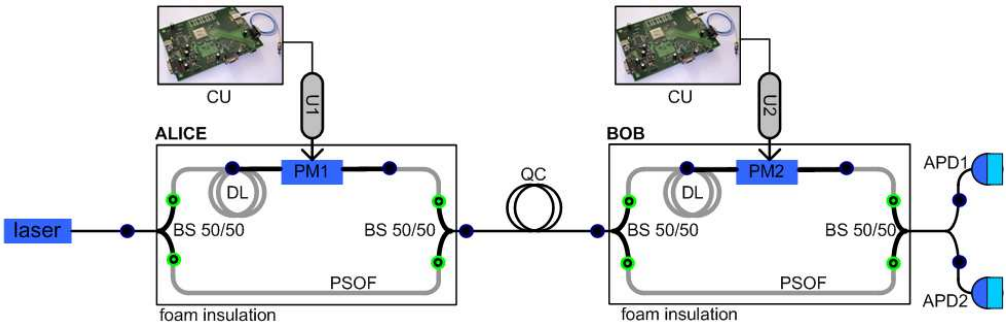

Fig 4.2 위상안정화 광섬유를 이용한 단일방향 양자암호 시스템 구성
(CU: Control Unit, BS: 3dB beamsplitter, DL: delay line, PM: phase modulator, Att: attenuator, QC: quantum channel, APD: avalanche photodiode)

앨리스와 밥의 간섭계는 Fig 4.2에서 보듯이 ±0.01℃의 정밀한 온도 보정 시스템 없이 온도 변화를 최소화 하기 위해서 단열재를 이용하여 insulation을 하게 된다.

제 4.3 절 Single Photon Counter Module (SPCM)

이상적인 단일광자 검출기는 단일광자가 검출기에 입사될 경우 전기적 논리 신호를 발생해야 한다. 그러나 실제로 단일광자 검출기로서 APD를 사용할 경우에는 단일광자가 입사해도 전기적 신호를 발생 못할 수도 있다. 입사된 광자의 양자 효율 (quantum effieciency)은 확률적으로 100% 이하가 된다. 또한 단일광자가 입사하지 않을 경우라도 캐리어의 thermal generation (dark noise)에 의해 전기적 신호가 발생할 수도 있다. 이는 또한 APD junction에 갖힌 전하에 의해서도 발생할 수 있다 (afterpulse). Dark noise는 APD 소자 냉각을, afterpulse noise는 적정한 geiger pulse mode 사용으로 해결 할 수 있다.

Dark noise의 측정은 암실에서 실행했으며 밥의 Laser (1550nm)는 동작시키지 않는다. APD는 열전소자를 이용하여 Fig 4.3과 같은 구성으로 -60℃까지 냉각하게 된다. 효율적인 냉각을 위해 Fig와 같이 동판을 사용하여 열전소자의 열을 방출해 주며 APD 내부 공간에 form을 채워넣어 단열을 하였다. Geiger mode gate pulse는 0.5 와 1 MHz의 frequency (f_G), 3 ns pulse width, 4.2 V의 pulse amplitude로 동작하게 되며 (Fig 4.5) 이 gate pulse는 DC bias voltage와 함께 APD에 인가되게 된다. 단일광자의 입사 없이 -60℃에서 thermal generation에 의한 전기적 신호는 frequency counter를 이용해서 count (f_D)하게 된다. gate pulse당 dark count probability (P_D)는 아래와 같이 계산 된다.

$$P_D = \frac{f_D}{f_G} \tag{4-1}$$

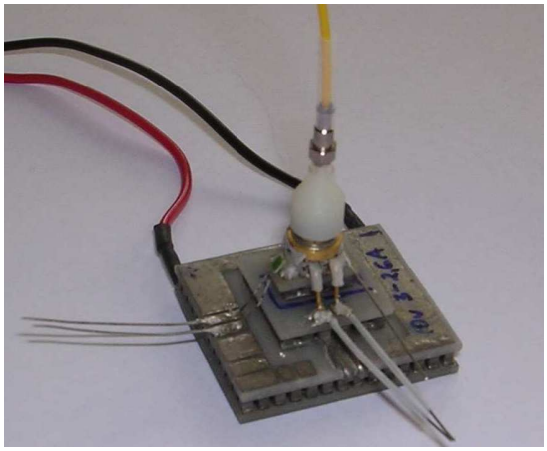

Fig 4.3 열전소자와 APD 구성

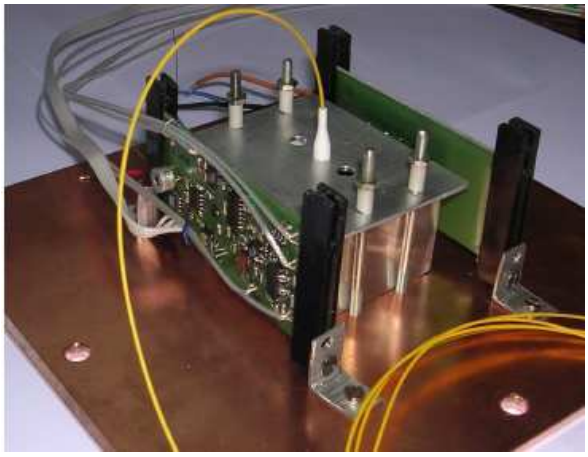

Fig 4.4 SPCM

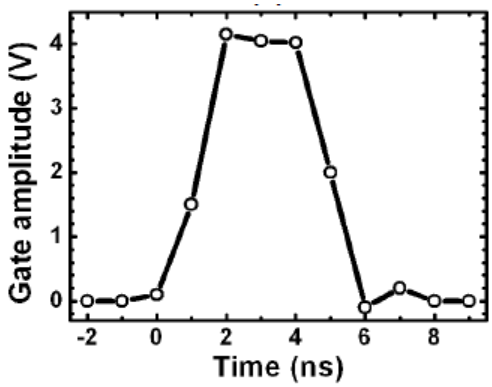

Fig 4.5 Geiger mode gate pulse

Reverse bias voltage의 변화에 따라 P_D의 측정값을 Fig 4.6과 같다. 단일광자를 검출하기 위해서는 P_D를 최소화해야 한다. 이에 알맞은 reverse bias는 42V이며 이때의 dark count probability (P_D)는 10^{-5}~10^{-4} 정도가 된다. 10^{-5}의 PD는 QBER<15% 조건을 충분히 만족할 수 있는 수치이다. QBER이 15% 이하가 되면 일반적으로 error collection algorithms을 통해 양자키 분배를 할 수 있게 된다. 그러나 error collection은 양자키를 공개하는 것을 기반으로 하기 때문에 QBER이 증가할 수록 양자키가 도청당할 확률도 증가하게 된다. QBER에 대해서는 다음 장에서 자세히 설명하겠다.

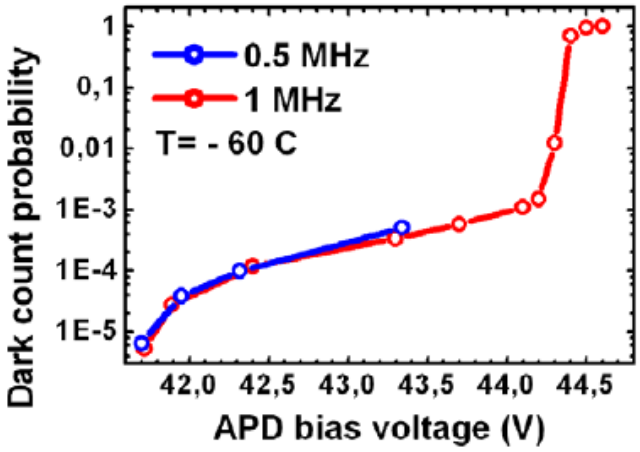

Fig 4.6 bias voltage에 따른 P_D

SPCM의 양자효율 (quantum efficiency)을 측정하기 위해서 dark count 측정에서 사용된 geiger mode gate pulse를 동작 시키고 laser를 동작 시켜 광신호가 APD에 입사될 때의 시간을 gate pulse와 동기화 시켜준다. laser 출력단에서 측정된 average output power P를 0.5 또는 1μW가 유지되게 고정한다. 이때 laser pulse에 해당되는 mean photon number는 아래의 식과 같다.

$$\mu = \frac{P}{\hbar w f_L} \qquad (4\text{-}2)$$

$\hbar w$는 1550nm 파장의 photon energy를 의미하며 식 4-2에 의해 μ는 laser pulse 당 평균 10^7개의 광자수를 포함하게 된다. laser diode의 출력단에 pigtail fiber에 attenuator를 연결하여 80dB를 감쇄하게 되면 laser pulse 당 평균 광자수 (μ)는 0.1이 된다. 이렇게 감쇄를 하여 확률적으로 단일광자를 생성하는 것은 Poisson distribution에 의해서 P_0=0.905, P_1=0.0905, $\sum P_{n>1}$=0.0045가 된다. 이는 laser pulse에 two photon 이상이 생길 확률이 0.45%라는 의미로 real single photon source와 비교하여 무시할 수 있는 수치이다. 이러한 이유로 보통 감쇄하여 확률적으로 생성된 단일광자를 pseudo single photon이라 한다. 80dB attenuator의 출력은 광섬유를 통해 SPCM으로 연결되며 이는 다시 frequency counter에서 측정하게 된다. Fig 4.7은 상기 조건으로 구성하여 측정된 단일광자 검출 파형을 나타낸다.

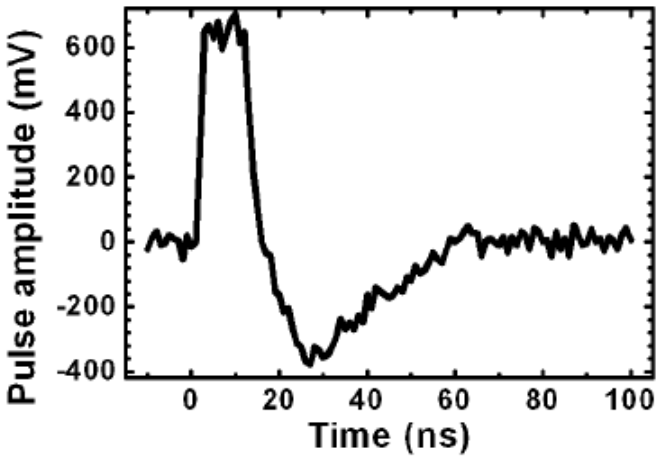

Fig 4.7 단일광자 검출 파형

이전에 측정한 PD와 감쇄하여 생성된 단일광자를 APD에 입사하여 측정한 f_C와 함께 식 4-3을 이용하여 quantum efficiency를 계산할 수 있다.

$$\eta = \frac{1}{\mu}\left[\frac{f_C}{f_L} - P_D\right] \qquad (4\text{-}3)$$

0.5, 1MHz 의 주파수로 laser와 geiger mode를 동작시키고 APD를 -60℃ 냉각한 조건에서 APD bias volatage에 따른 quantum efficiency는 Fig 4.8과 같다. APD를 이용한 단일광자 검출을 위한 최적 조건을 구하기 위해 Fig 4.6과 Fig 4.8으로부터 SPCM의 dark count probability와 quantum efficiency를 결정해야 하며 이는 Fig 4.9와 같다. 두 항목은 모든 양자암호시스템의 전송거리, 전송속도를 평가할 수 있는 중요한 지표이다. Fig 은 Plug & Play system을 개발한 스위스 Gisin 연구진의 SPCM 성능과 우리 시스템의 SPCM 성능을 비교해 보았다. Gisin 연구진은 동일한 APD(JDS Uniphase, ETX 40 APD END BA)를 사용하였으며 10KHz frequency, 2.4ns gate pulse width, -60℃ 조건에서 측정한 결과이다. 우리 SPCM의 성능은 Gisin 연구진의 성능과 가까운 수치를 나타내며 이로써 전송거리와 속도면에서 향상된 성능의 양자암호시스템을 예상할 수 있다.

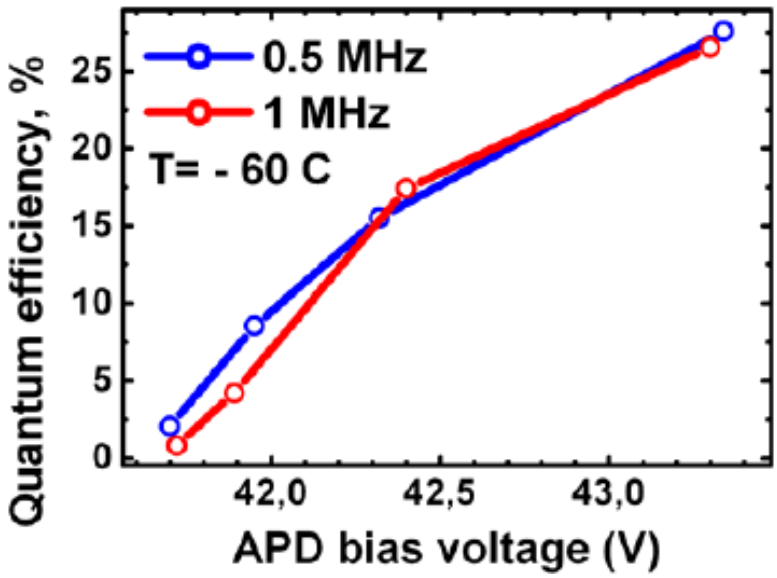

Fig 4.8 APD bias에 따른 quantum efficiency

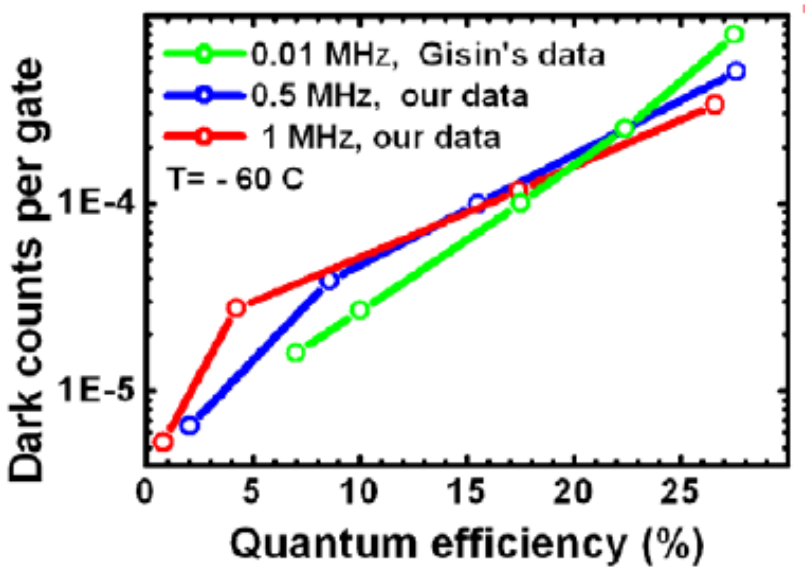

Fig 4.9 Quantum efficiency vs. Dark counts probability

Afterpulse noise는 앞에서 설명했듯이 APD junction에 갖힌 전하에 의해서 단일광자가 입사되지 않은 상태에서 전기적 신호를 발생시키는 것으로 SPCM의 성능과 단일광자 검출 속도에 영향을 미치는 중요한 변수이다. Afterpulse probability P_A는 APD 소자 온도가 낮아질수록 그리고 이전에 발생한 avalanche와의 time delay 가 작아질수록 증가하는 경향이 있다. P_A의 측정은 우선 laser pulse의 반복주기를 100 kHz (10us space between laser pulse)로 한다. 100kHz의 반복주기는 afterpulse effect를 줄이기 충분하다. 다음으로 laser output power를 1μW로 고정하고 40dB attenuator를 이용하여 laser pulse 당 평균 광자수(μ)를 20으로 유지한다. Attenuator의 출력은 SPCM에 연결한다. 앞에서 측정한 quantum efficiency(η)가 5~20%임을 고려하면 평균 광자수(μ)가 20일때 검출 효율은 100%가 나오게 된다. 다시말해 output pulse frequency는 laser pulse frequency(f_L)와 같게 된다. 이와 같은 측정을 반복해서 하게 되는데 laser pulse space를 0.1~10μs로 변화를 주면서 측정을 한다. 변화된 laser pulse space에 따라서 afterpulse probability는 식 4-4와 같다.

$$P_A = \frac{f_A}{f_L} - P_D \qquad (4\text{-}4)$$

식 4-4를 이용하여 APD 소자 온도의 변화와 pulse space 변화에 따른 afterpulse probability는 Fig 4.10과 같다. Afterpulse probability는 온도와 pulse space가 줄어들수록 높아지는 경향을 보이며 Gision 연구진의 결과와 비슷한 측정값을 보이고 있다.

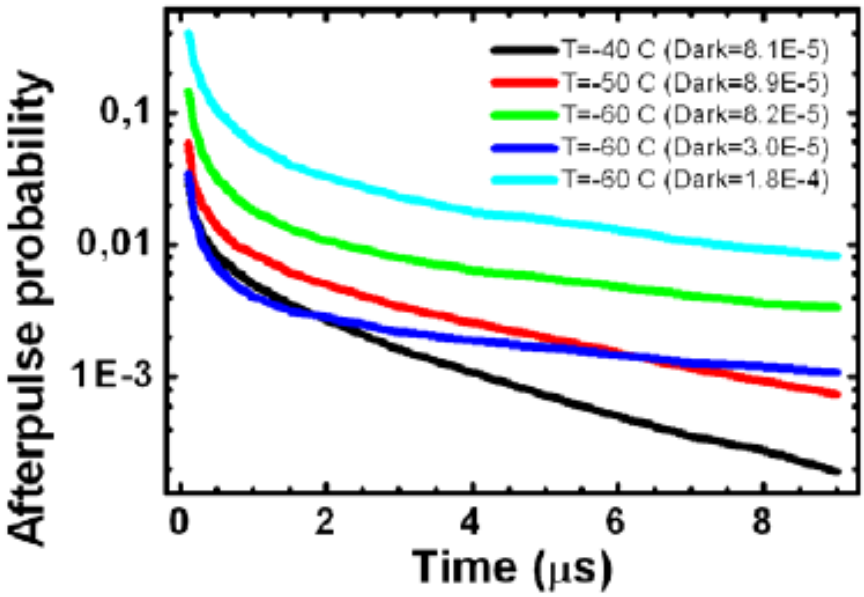

Fig 4.10 Afterpulse probability with variation of pulse space and temperature of APD

제 5 장 실험 결과

제 5.1 절 시스템 안정성

5.1.1 단순 간섭 실험

일반 광섬유의 열팽창 계수는 약 6ppm/℃이다[27]. 이 열팽창 계수로 인해 광섬유 기반으로 간섭계를 구성하였을 때 위상 변이와 전달 지연이 생기게 된다. 위상 변이와 전달 지연은 간섭계의 두 경로를 지나는 두 신호의 위상 차이에 변화를 주어 간섭되는 신호가 출렁이는 현상을 보이게 된다. Fig 5.1은 단일모드 광섬유를 이용하여 Mach-Zehnder 간섭계를 구성하였을 때 측정된 간섭 신호의 변화이다. 만약 단일모드 광섬유를 이용하여 단일방향 양자암호 시스템을 구성한다면 키 분배는 사실상 불가능하게 된다. 그래서 여러 연구진은 정밀한 온도 제어 시스템을 이용하는 방법과 위상 변조 값을 위상변이에 맞춰서 보상해 주는 방법 등을 사용해서 안정성을 확보하였다[11][24]. 그러나 안정성이 확보된 상태에서 키 분배 시간은 1~2분 내외에 불과하다[11].

위상안정화 광섬유의 열팽창 계수를 측정하는 대신 동일한 경로를 가진 Mach-Zehnder 간섭계를 위상안정화 광섬유를 이용하여 구성한 다음 그 출력 파형을 측정하였다. 간섭계는 Fig 4.2와 같이 구성된다. Laser, 3dB beamsplitter, SPCM으로 구성되며 위상안정화 광섬유는 두 경로에만 적용하였다. SPCM은 geiger mode를 사용하지 않고 breakdown 이하의 전압을 인가하였다. Insulation은 약 2 cm 두께를 갖는 스티로폼 박스를 이용하였다.

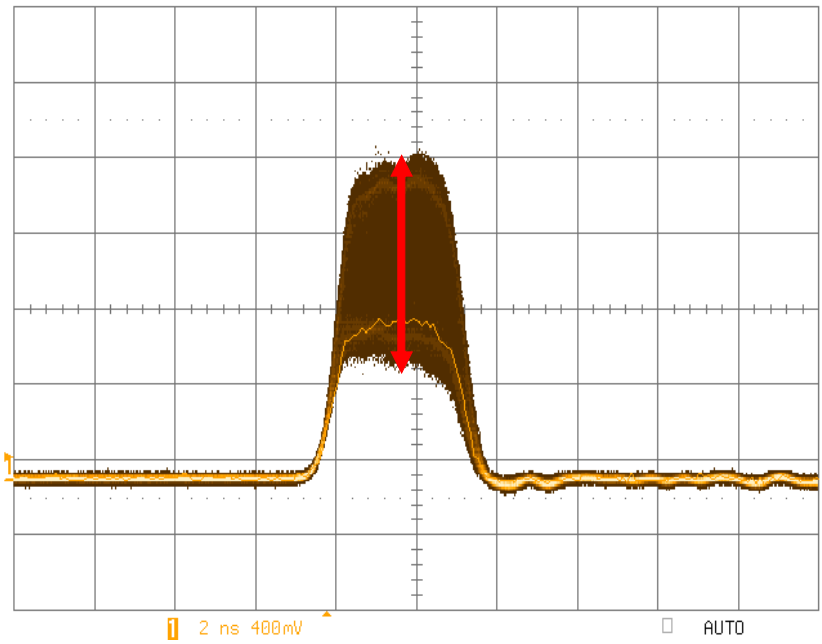

Fig 5.1 위상변이로 인해 변하는 간섭 신호

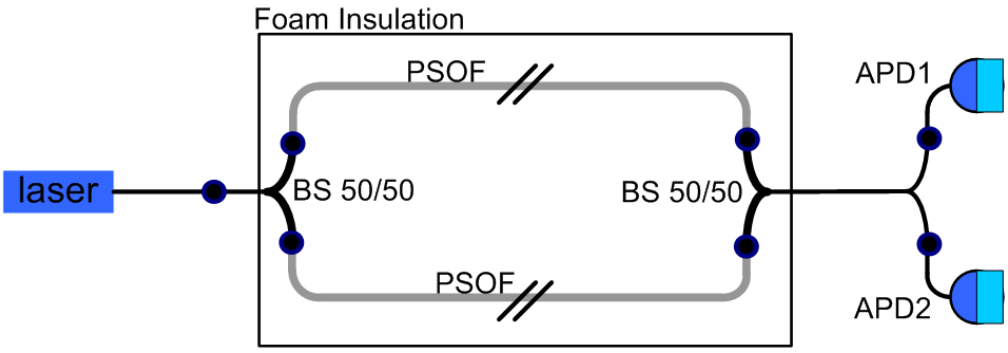

Fig 5.2 동일한 두 경로를 갖는 Mach-Zehnder 간섭계

(BS: beamsplitter, APD: avalanche photodiode)

condition	SMF No insulation	SMF Insulation	PSOF No insulation	PSOF Insulation
Standard deviation	6.3%	5.4%	3.2%	2.9%

Table 5.1 간섭 신호의 변화

Table 5.1은 Fig 5.2의 실험 구성으로 간섭 신호의 출력 파형 세기 변화를 나타낸 것으로 평준화한 출력신호의 표준편차를 나타낸 것이다. 간섭계 두 경로에 단일모드 광섬유와 위상안정화 광섬유를 적용한 경우와 온도조건으로 상온과 단순단열 상태, 총 4가지 경우의 출력 파형의 세기 변화를 측정하였다. 상온 조건은 단열재 없이 간섭계 부분을 완전히 개방한 상태를 말하며, 단열 조건은 단순 단열재를 이용하여 온도 제어 시스템 없이 간섭계 부분을 단열한 조건을 의미한다. 단일모드 광섬유/상온 조건의 간섭 신호의 크기는 출렁임이 심하여 각 샘플 값의 표준 편차가 평균 출력(100%) 신호의 6.3% 비중으로 측정되었다. 단일모드 광섬유/단순단열 조건의 간섭 신호 크기는 상온 조건과 비교하여 안정적이었으며 표준편차는 5.4%를 나타냈다. 위상안정화 광섬유/상온 조건은 단일모드 광섬유/단열 조건의 표준 편차보다 더 안정적으로 3.2%를 나타내었다. 위상안정화 광섬유의 출력 신호가 단일모드 광섬유의 출력 신호 보다 작은 이유는 위상안정화 광섬유의 특성으로 감쇄율이 2dB/m를 나타내기 때문인데 단일모드 광섬유가 약 0.2 dB/km인 것에 비하면 상당히 큰 감쇄율을 보이고 있다. 위상안정화 광섬유/단열 조건에서는 표준편차가 2.9%로 가장 안정적으로 나왔다. 상기 실험을 통해서 단일방향 양자암호 시스템을 위상안정화 광섬유/ 단열 조건으로 구성한다면 정밀한 온도 제어 시스템 없이 시스템을 구축할 수 있을 것으로 간접적으로 예상이 되며 Plug & Play system의 자동 위상 보정 수준의 안정성을 확보할 수 있을 것으로 예상이 된다. 단점으로는 위상안정화 광섬유의 감쇄율이 2 dB/m로서 단일모드 광섬유에 비해서 상당히 크다는 것인데, Fig 4.2에서 앨리스 부분은 광신호가 attenuator에 입력되기까지 다광자를 이용하기 때문에 문제가 없다. 그러나 단일광

자로 감쇄되어 밥에 전송되어서는 위상안정화 광섬유의 감쇄율이 단일광자 전송에 제약을 주게 된다. 이는 간섭계 경로의 길이를 최소화하여 해결할 수 있다.

5.1.2 위상 변이

위상 변이의 측정은 Fig 4.2의 실험 구성으로 실행하였으며 비대칭 간섭계 구간을 단열재를 이용하여 단열하였다. 광섬유는 물리적 진동을 제거하기 위해 단열 케이스 내에 고정하였다. 광원은 다광자를 사용하였으며 attenuator와 quantum channel은 실험 구성에서 제외하였다. SPCM은 geiger mode가 아닌 breakdown 전압 이하의 bias를 인가하여 측정하였다. 위상 변조 전압은 -5~5V으로 조정하였으며 digital delay generator (Stanford Research System, DG535)를 이용하여 위상 변조 신호의 타이밍을 조절하였다. 위상 변이를 측정하는 방법은 다음과 같다. SPCM의 한쪽 APD 출력 신호를 측정하면서 PM1과 PM2의 위상 변조 전압을 조절하면 APD 두 출력 신호의 최대 출력이 나오는 변조 전압 값을 찾을 수 있게 된다. 이때 시간이 변함에 따라 변하는 간섭 신호를 측정한다. 일정 시간 동안 변한 간섭 신호를 PM1 또는 PM2의 위상 변조 전압을 조절하여 출력 간섭 신호를 다시 최대로 맞추게 된다. 최대로 맞출 때 변조 전압의 차이를 기록하여 phase modulator의 V_{π} 와 비교하여 측정 시간과 함께 위상 변이를 유추할 수 있게 된다.

Fig 5.3는 시간에 따라 측정된 위상 변이를 나타낸다. 위상 변이는 평균 0.00153 π/sec, 최대 0.0024 π/sec으로 측정되었다. 지금껏 다른 연구진의 단일방향 시스템에서 보고된 위상 변이는 0.00318 π/sec (최대값)이 보고된 바 있으며 최근에는 상당히 안정된 0.00027 π/sec (최대값)이 보고된 바 있다[24][11]. 0.00027 π/sec 의 위상 변이를 갖는 시스템은 몇 분 동안 양자키 분배 과정을 수행할 수 있다. 이 두 시스템은 특별한 재료를 이용한 단열재와 정밀한 온도 제어 시스템을 이용하여 단일모드 광섬유를 이용한 시스템에서 위상 안정성을 확보하였다. 본 논문에 제안된 시스템은 최근 보고된 위상 변이의 수치보다는 안정적이지 못하지만 온도 제어 시스템을 이용하지 않고 단순 단열재를 이용한 단열 조건에서 위상안

정화 광섬유를 이용하여 안정성을 유지했다는 점에 주목할 만하다. 또한 본 시스템의 측정치는 0.00318 π/sec을 보고한 바 있는 시스템 보다 더 안정적인 것을 감안할 때, 앞으로 Plug & Play 시스템의 안정성을 유지할 수 있을 것으로 예상된다. 또한 정밀한 온도 제어 시스템을 사용하지 않았다는 점, 단순 단열재를 사용했다는 점을 고려한다면 앞으로 안정성을 더욱 확보하여 상업적으로도 충분한 가능성이 있다고 생각한다.

위상 변이 안정성 향상을 위해서는 다음과 같은 사항을 고려할 수 있다. 첫째, 앨리스, 밥의 간섭계에 사용된 단일모드 광섬유와 편광유지 광섬유의 사용 비율을 낮춰야 한다. 현재 간섭계의 위상안정화 광섬유가 사용되지 않은 부분은 Fig 4.2에서 앨리스 부분에서 BS1의 출력 부분 pigtail 단일모드 광섬유로 15cm, PM1의 양단 pigtail 편광유지 광섬유 2m, BS2의 입력 부분 pigtail 단일모드 광섬유로 15cm를 사용했으며, 밥에서도 동일하다. 특히나 phase modulator의 pigtail 편광유지광섬유의 길이를 최소화해야 한다. 둘째, 특별한 단열재를 이용한 단열 방법도 안정성 향상에 기여할 수 있다. 본 시스템은 광학계를 스티로폼 케이스 안에 위치하여 단열을 했으나 진공 상태 또는 모래와 같은 것을 사용하여 단열을 한 시스템도 보고되고 있으며 단순 단열재를 사용한 것보다는 안정성이 향상될 것으로 보인다. 셋째, 양자암호 키 분배 과정 전에 앨리스와 밥이 위상 변이를 측정하여 이를 보상하는 방법이 있다. 이는 시간에 따라 변하는 위상 변이를 예측하여 앨리스와 밥의 위상 변조 전압에 보상하여 키 분배를 하는 것이다.

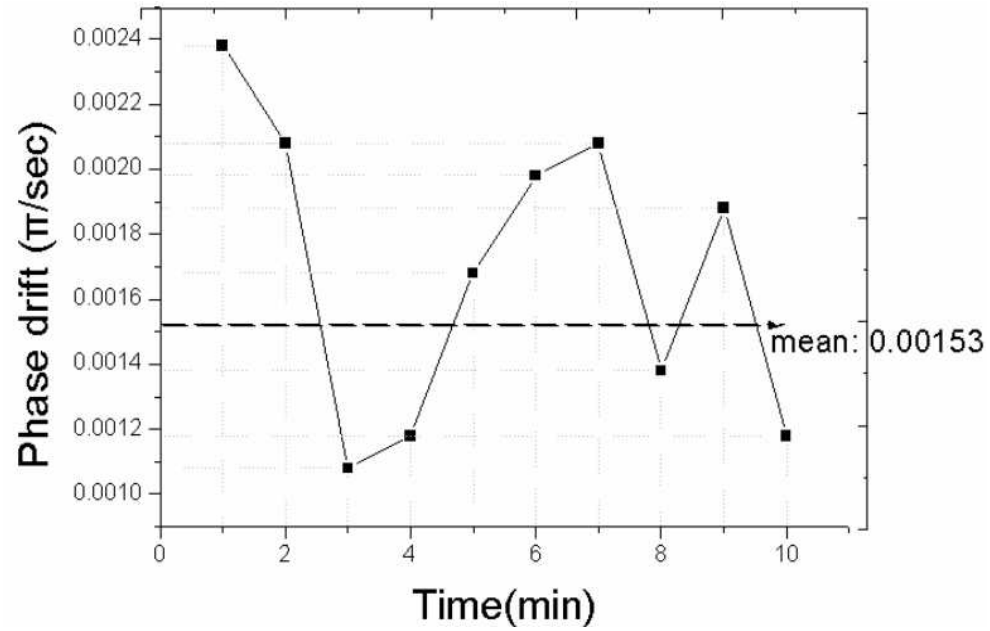

Fig 5.3 시간에 따른 위상변이

5.1.3 Visibility

Visibility는 Mach-Zehnder 간섭계를 기반으로 구성된 광학계에 근거한 노이즈 특성을 나타낸다. 보강과 상쇄간섭의 정도차이를 나타내는 것으로 visibility가 클수록 간섭계는 안정적인 간섭을 하게 된다. 간섭계의 잘못된 구성으로 인한 노이즈는 양자암호 시스템의 가장 큰 노이즈로 작용할 수 있는 만큼 반드시 줄여야 한다.

Visibility를 측정하는 방법으로는 두 가지가 있다. Fig 4.2에서 다광자를 사용하는 방법과 3~4 광자를 사용하는 방법이 있다. 다광자를 이용할 때는 밥의 APD에서 출력 신호의 크기를 이용하여 구하게 되며 3~4 광자를 사용할 경우에는 APD를 geiger mode로 동작하여 검출 신호를 카운트하게 된다. 본 측정 실험에서는 3~4 광자를 사용하여 visibility를 측정하였다. 측정 방법은 다음과 같다. Fig 4.2의

실험구성에서 Laser는 1ns의 펄스 폭과 1Mhz의 주기를 갖는 신호를 이용하여 작동한다. Digital delay generator를 이용하여 PM1의 timing을 조정하며 변조 신호는 -5~5V를 가변하여 인가한다. 앨리스에서 양자채널에 들어가기 전의 광출력은 1 μW가 되도록 laser pulse를 조절한다. Attenuator는 50dB를 이용하여 2~3 광자를 생성한다. 양자채널은 0km, 15km, 25km를 각각 적용한다. 밥에서도 앨리스와 마찬가지로 digital delay generator를 이용하여 PM2에 -5~5V의 변조신호를 timing을 조정하여 인가한다. SPCM은 열전소자를 이용하여 APD를 -60℃까지 냉각하며 geiger mode로 동작하게 된다. Geiger mode의 펄스는 2ns의 펄스 폭과 1V의 크기를 갖는 신호를 이용한다. APD에 광자가 도착하는 timing과 geiger pulse의 동기화는 digital delay generator를 이용하여 조정한다. 이후 PM1과 PM2의 전압을 조정하여 위상변조 8가지 경우에 대해서 APD1 과 APD2에서 검출을 하여 카운트의 최대값과 최소값을 구하게 된다. 이를 평균하여 식 5-1을 이용하여 visibility를 구한다.

$$Visibility = \frac{f_r - f_w}{f_r + f_w} \qquad (5\text{-}1)$$

f_r은 위상변조에 따라 검출되는 광자의 카운트를 의미하며, f_w는 위상변조와 다르게 검출되는 카운트를 의미한다. 각각의 카운트는 f_D dark count를 포함하지 않게 된다. 위 식을 이용하여 양자채널에 따른 visibility를 Fig 5.4에 도시하였다.

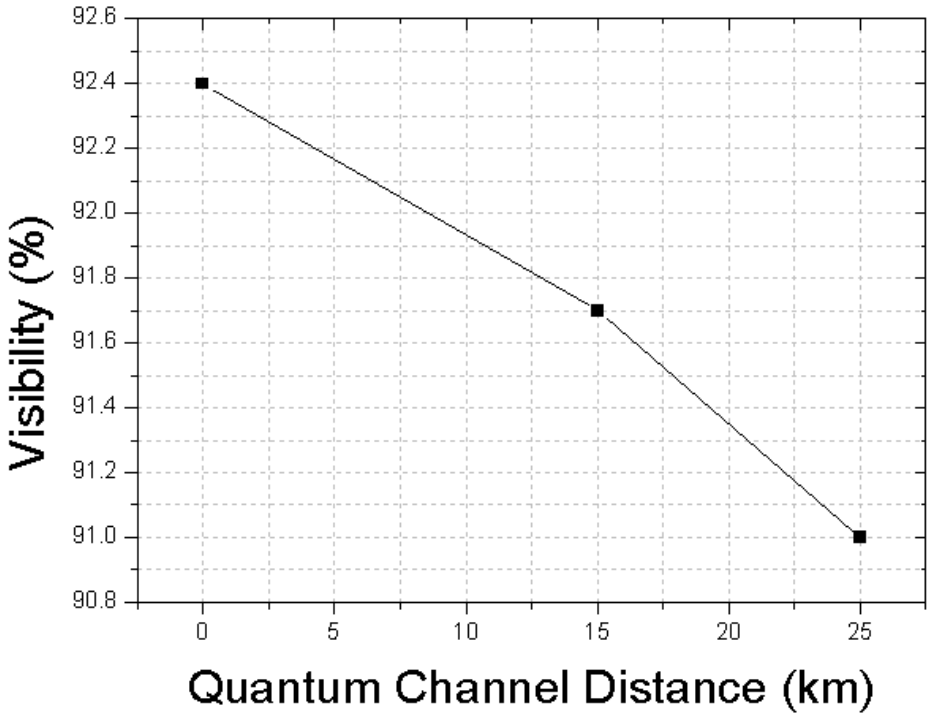

Fig 5.4 양자채널에 따른 Visibility

앨리스와 밥을 직접 연결한 시스템에서는 92.4%의 visibility가 측정되었다. Gisin 연구진의 Plug & Play 시스템은 99.6~99.7%의 visibility를 보였으며 보통 98% 이상의 visibility가 허용수치이나 제안된 시스템은 상대적으로 낮은 visibility를 나타내고 있다. 높은 visibility를 위해서는 비대칭 간섭계 입출력 포트의 편광축 설정을 정확히 해야 한다. 그러나 제안된 시스템의 구현은 위상안정화 광섬유를 사용하기 위해서 광융착접속기를 사용함으로써 편광축 보정을 고려하지 못했다. 이러한 이유로 낮은 visibility를 보인 것으로 보인다. 또한 식 5-1에 따라 visibility는 양자채널의 거리와 독립적이어야 한다. 그러나 실험결과는 양자채널이 증가함에 따라 visibility가 감소하는 것으로 보였다. 92.4%(0km)와 91%(25km)는 비교적 많은 차이는 아니지만 위상변이가 원인으로 보인다. Visibility의 향상은 추후 정확한 편광축 설정으로 해결할 수 있다.

제 5.2 절 Quantum Key Parameter

지금까지 양자암호시스템의 성능 중 위상안정화 광섬유를 사용함에 있어서 안정성과 관련된 측정을 살펴보았다. 양자암호시스템의 키 분배에 관한 성능은 크게 세가지, sifted key rate, sifted key error rate, quantum bit error rate로 나눌 수 있다[9].

5.2.1 Sifted key generation rate

Sifted key generation rate는 양자암호 프로토콜을 수행한 후에 생성된 양자키의 생성 속도를 의미한다. 모든 양자암호시스템은 식 5-2으로 sifted key generation rate를 구할 수 있다. 1/2은 BB84 protocol factor이며 밥에서 2가지의 측정 편광을 사용하기 때문이다. f_L은 레이저 펄스 발생 속도이며 μ은 펄스당 평균 광자수, η은 quauntum efficiency, T는 단일광자가 전송되는 시점에서부터의 감쇄정도를 나타낸다.

$$R_{sift} = \frac{1}{2} f_L \mu \eta T \qquad (5\text{-}2)$$

5.2.2 Sifted key error rate

Sifted key error rate는 양자암호 프로토콜을 수행하여 키를 생성하면서 생기는 에러 속도를 나타낸다. 이는 간섭계의 부정확성으로 인한 에러와 검출기의 에러로 나타낼 수 있으며 식 5-3과 같다.

$$R_{err} = \frac{1-V}{2} R_{sift} + \frac{1}{2} f_L P_D \qquad (5\text{-}3)$$

5.2.3 quantum bit error rate

Quantum bit error rate는 양자암호 프로토콜을 수행하여 양자키를 생성하면서

생기는 전체적인 에러의 비율을 의미한다. 에러는 visibility와 연관된 간섭계의 부정확성에 기인한 에러와 단일광자검출기의 dark noise로 나타낼수 있으며 식 5-4와 같다. Dark noise는 작은값으로 무시하여 visibility만으로 QBER을 근사화할 수 있다[28]. Table 5.2 는 식 5-2~4 을 이용하여 전송채널의 거리, 평균 광자수에 따라서 제안된 시스템의 sift key 생성 속도와 QBER을 구한 것이다.

$$QBER = \frac{R_{err}}{R_{sift} + R_{err}} \approx \frac{1-V}{2} + \frac{P_{dark}}{\mu \eta T} \approx \frac{1-V}{2} \tag{5-4}$$

QC	25km		50km	
T	0.107		0.088	
μ	0.1	0.2	0.1	0.2
R_{sift}	802 bps	1.6 kbps	660 bps	1.32 kbps
R_{err}	76 bps	112 bps	69 bps	99 bps
QBER	9.4 %	6.9 %	10.5 %	7.5 %

Table 5.2 양자암호 키 분배 parameter

(f_L=1MHz, P_D=8 · 10^{-5} c/gate, η=15%, Visibility=0.91)

양자채널 25Km에서 0.1 photon의 평균 광자수를 사용하였을때 sift key rate는 802 bps를 나타냈으며 이때의 QBER은 9.4%를 나타냈다. 9.4%의 QBER 중에 반은 낮은 visibility 때문에 발생한 에러값이다. 일반적으로 양자암호시스템의 QBER은 10~15% 이내로 허용하고 있으나 측정된 값은 허용 QBER에 거의 가까운 값을 나타내고 있어 추후 계속된 실험에서 광학계의 정확한 정렬이 필요로 할 것으로 보인다. 양자암호 키 분배를 한 후에는 에러를 보정하기 위해서 error collection이라는 과정을 거친다.[13] Error collection은 양자키의 에러를 보정하기 위해서 특정

한 알고리듬에 따라 양자키 값의 일부분은 공개하는 것을 기반으로 한다. QBER이 높을 수록 공개하는 양자키의 비율은 증가하며 동시에 공개채널을 통해 도청이 되어 키 값이 유출될 가능성이 커지게 된다. 측정된 QBER로 보아 50Km까지 전송이 가능할 것으로 보인다.

제 6 장 결론

본 논문에서는 단일방향 구조의 양자암호 시스템 안정성 향상을 위해서 위상 안정화 광섬유를 적용한 단일방향 양자암호 시스템을 제안한다. 양자암호시스템의 기본 구조인 단순 간섭계를 구현하여 위상안정화 광섬유의 안정성의 특성을 파악하였으며 비대칭 Mach-Zehnder 간섭계 구간에 위상안정화 광섬유를 적용하여 정밀한 온도 제어 시스템 없이 단순 단열을 통해 단일방향 양자암호 시스템을 구현하였다. 또한 단일광자검출기를 구현하여 이의 특성을 파악하였다. 위상 변이는 평균 0.00153 π/sec, 최대 0.0024 π/sec가 측정 되었으며 이는 0.00027 π/sec의 위상 변이를 보인 다른 연구진의 결과와 비교하여 불안정한 결과이지만 여타 연구진의 단일방향 시스템의 위상 변이보다는 안정한 결과이다. 간섭계 구성에 전체적으로 위상안정화 광섬유를 사용하지 않았다는 점에서 볼 때 정교한 광학계 구성과 단열을 통해 plug & play 수준의 안정성을 단일방향 시스템에서 보일 수 있을 것으로 기대 되며 나아가 상용화 수준의 시스템 제작이 가능할 것으로 예상된다. 구현된 시스템의 간섭계 정확성을 측정하기 위해서 visibility를 측정하였으며 전송거리 25km에서 91%의 visibility를 나타내었다. 또한 측정 parameter를 근거로 하여 전송채널 25Km 상에서 R_{sift} = 809 bps, QBER = 9.4 %, 전송채널 50Km 상에서는 R_{sift} = 660 bps, QBER = 10.5 %를 나타냈다.

참고문헌

[1] D. Davies, "A brief History of Cryptography", Information Security Technical Report. Vol. 2, No. 2 pp. 12-17, 1997

[2] W. Diffie, and M. E. Hellman, "New directions in cryptography", IEEE Trans. Inf. Theory. IT-22, pp. 644-654, 1976

[3] G. Vernam, "Cipher printing telegraph systems for secret wire and radio telegraphic communications", J. Am. Inst. Electr. Eng. Vol. **45**, pp. 109-115, 1926

[4] R. L. Rivest, A. Shamir, and L. M. Adleman, "A method of obtaining digital signatures and public-key cryptosystems", Commun., ACM **21**, pp. 120-126, 1978

[5] P. W. Shor, *Proceedings of the 35th Symposium on Foundations of Computer Science*, pp. 124 – -134, 1994

[6] J. L. Massey, "Introduction to Contemporary Cryptography", Proceedings of the IEEE, Vol. 76(5), pp. 533, 1988

[7] Bennett, C. H., and Brassard, G., "Quantum cryptography : Public key distribution and coin tossing", 1984, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, pp. 175-179

[8] Charles H. Bennett et al., "Experimental Quantum Cryptography", Journal of Cryptology, No. 5, 1992

[9] Nicolas Gisin, Gregoire Ribordy, Wolfgang Tittel, Hugo Zbinden, "Quantum Cryptography", Reviews of Modern Physics, Vol. 74, pp. 145-195, Jan. 2002

[10] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster and J. G. Rarity, "Quantum cryptography: A step towards global key distribution", Nature, Vol. 419, pp. 450, 2002

[11] C. Gobby, Z. L. Yuan, A. J. Shields, "Quantum key distribution over 122 km of standard telecom fiber", Appl. Phys. Lett., Vol. 84, pp. 3762-3764, 2004

[12] 노태곤, 김헌오, 홍종철, 윤천주, 성건용, "양자암호통신 기술“, 전자통신동향분석, Vol. 20, No. 5, pp. 70-83, 2005

[13] N. Lutkenhaus, " Security against eavesdropping in quantum cryptography", Phys. Rev. A 54, pp. 97-111, 1996

[14] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states", Phys. Rev. Lett., Vol. 68, pp. 3121-3124, 1992

[15] Charles H. Bennett, Gilles Brassard, Artur K. Ekert., "Quantum Cryptography", Scientific American, Vol. 267, pp. 50-57

[16] A. Muller, J. Breguet and N. Gisin, "Experimental demonstration of quantum cryptography using polarized photons in optical fiber over more than 1 km", Europhysics Letters, Vol. 23, pp. 383-388, 1993

[17] A. Muller, H. Zbinden and N. Gisin, "Underwater quantum coding", Nature, Vol. 378, pp. 449-449, 1995

[18] A. Muller, H. Zbinden, and N. Gisin, "Quantum cryptography over 23 km in installed under-lake telecom fibre", Europhysics Letters, Vol. 33, pp. 335-339, 1996

[19] J. D. Franson and B. C. Jacobs, "Operational system for Quantum cryptography", Elect. Letters, Vol. 31, pp. 232-234, 1995

[20] T. Okoshi, "Polarization-State Control Schemes for Heterodyne or Homodyne Optical Fiber Communications", Journal of Lightwave Technology, Vol. LT-3, No. 6, pp. 1232-1237, 1985

[21] Wolfgang Tittel, Gregoire Ribord and N. Gisin, "Quantum Cryptography", Physics World, Vol. 11, No. 3, pp.41-46, 1998

[22] P. D. Townsend, J. G. Rarity and P. R. Tapster, "Single photon interference in 10 km long optical fibre interferometer", Electronics Letters, Vol. 29, No. 7, pp. 634-635, 1993

[23] P. D. Townsend, "Secure key distribution system based on quantum cryptography", Electron Letters, Vol. 30, pp. 809-811, 1994

[24] C. Marand, P. D. Townsend, "Quantum key distribution over distances as long as 30 km", Optics Letters, Vol. 20, pp 1695-1697, 1995

[25] P. D. Townsend, “Quantum Cryptography in optical fiber networks", Optical Fiber Technology, Vol. 4, pp. 345-370, 1998

[26] Martinelli M., "A universal compensator for polarization changes induced by birefringence on a retracting beam", Optical Communication, Vol. 72, pp. 341-344, 1989

[27] T. Naito, K. Ebihara, M. Suetake, E. Ezura, "RF reference distribution using fibre-optic lins for KEKB Accelerator", Proc. Conf. Particle Accelerator, pp. 791-793, 2001

[28] H. Kosaka, A. Tomita, Y. Nambu, T. Kimura, K. Nakamura, "Single-photon interference experiment over 100 km for quantum cryptography system using balanced gated-mode photon detector", Electron. Lett., Vol. 39, pp. 1199-1201, 2003

ABSTRACT

One-Way Quantum Cryptography System Using Phase-Stabilized Optical Fiber

Park, Jun-Bum

Dept. of Electrical & Electronic Eng.

The Graduate School

Yonsei University

A One-Way Quantum Cryptography System, which is based on unbalanced time-division (time-multiplexing) interferometers and a Phase-Stabilized Optical Fiber (PSOF), is proposed in this paper. In contrast to the previous QKD system, the PSOF is used in this system without any precise temperature control system. A ~0.00238 π/sec phase drift was obtained. This drift is enough to perform a stable key distribution. If PSFO is adopted in the all of the unbalanced interferometer, this drift will be better. We also obtained the 91% of visibility. Concerning the key distribution parameter, 802bps of sift key rate and 9.4% of QBER were estimated in the condition of the 25km of quantum channel, 15% of quantum efficiency and 8×10^{-5} c/gate of dark count probability. In the case of the 50km of quantum channel, 606bps of sift key rate and 10.5% of QBER were estimated. From these records, it is possible to perform a key distribution in the 50km of quantum channel.

Key words : quantum cryptography system, phase stabilized optical fiber, quantum key distribution, shingle photon detection