논문 2007-44SC-3-8

Plug & Play 양자암호 시스템

(Plug & Play quantum cryptography system)

이 경 운*,**, 박 철 우**, 박 준 범**, 이 승 훈**, 신 현 준**, 박 정 호*, 문 성 욱**

(Kyung-Woon Lee, Chul-Woo Park, Jun-Bum Park, SeungHun LEE, Hyun-Jun Shin, Jung Ho Park, and Sung Wook Moon)

요 약

1550nm의 파장대를 이용하는 자동 위상보정 양자암호 시스템을 소개한다. 양자키 분배 시스템에서 자동위상보정된 양자키 분배를 위한 메인 컨트롤보드와 phase modulator를 제어할 수 있는 보드를 제작하였고, 단일광자검출기를 위한 dark count당 photon count, quantum key distribution rate(R_{sift})와 quantum bit error rate(QBER)값을 측정하였다. 이 시스템은 25km의 광섬유상에서 quantum bit error rate(QBER) 3.5%의 결과값을 얻었고, 이는 상용화가 가능할 것으로 예상된다.

Abstract

We present a auto compensating quantum key distribution system based on optical fiber at 1550nm. In the quantum key transmission system, main control board and phase modulation driving board are fabricated for auto controlling quantum key distribution(QKD). We tested the single photon counts per dark counts for a single photon detector, quantum key distribution rate(R_{sift}) and the quantum bit error rate (QBER). Quantum bit error rate of 3.5% in 25km QKD is obtained. This system is commercially available.

Keywords: Quantum cryptography, Single photon detection, Quantum key distribution, Quantum bit error rate

I. 서 론

인터넷과 고성능 컴퓨터의 급격한 보급과 함께 사회는 점차 네트워크화 되고 이를 통해 물품구매 등 전자상거래가 활발히 이루어지고 또한 지식, 정보 등의 자료들이 네트워크를 통하여 교환되고 있다. 사회는 이를 충족시키기 위해 고성능 컴퓨터의 개발을 촉진시켰으며 양자 통신, 양자 컴퓨터 등의 연구가 연구소 단위에서 본격화 되고 있다. 반면 국가의 비밀 정보를 다루는 국방 및 주요 국가기관이나 기업 및 금융기관 등은 보안문제가 큰 이슈가 되었다. 양자암호는 양자역학의 불확실성을 바탕으로 양자효과를 보이는 단일광자는 복제가 불가능하다는 점에 착안하여 1970년도에 Stephen Wiesner에 의해 처음 소개 되었고 C. Bennett에 의해 1979년 최초로 실험에 의해 입증되었다[1~2]. 최초의 양자암호 시스템은 30cm 전송거리의 자유공간에서 실험되었으며, 스위스의 Gisin연구진은 Faraday mirror를 이용한 왕복구조의 광섬유 기반 양자암호 시스템을 개발하였다[3]. 양자암호는 단일광자를 이용하여 통신하는 방식으로 수학적 기교가 아닌 물리적 양자현상을 이용해 도청을 원천적으로 막는 암호기술이다. 이 기술은 극도의 보안을 필요로 하는 국가기관이나 국방기관 및 금융기관에서 사용될 수 있으며, 나아가서는 개인 보안용 시스템으로까지 발전될 수 있을 것이다. 본 연구는 양자암호 시스템의 핵심 기술인 단일광자 감지시스템의 온도에 따른 특성에 대한 연구와 Plug and Play가 가능하도록 하는 컨트롤 보드를 이용한 양자키 분배에 관한 것이다.

* 고려대학교
(Korea University)
** 정회원, 한국과학기술 연구원
(Korea Institute of Science and Technology)
접수일자: 2006년8월10일, 수정완료일: 2007년4월20일

Ⅱ. Plug & Play 양자암호 시스템

1. 단일광자 감지모듈

단일광자 검출 소자로는 상용 광통신에서 사용되는 InGaAs APD를 사용하였다. 단광자에 의한 한 쌍의 전자 전공 쌍이 발생할 경우 1.6×10-19C이 발생한다. 일반적인 전자회로를 이용한 검출은 현실적으로 불가능하다. APD의 breakdown 특성을 이용하여 단광자를 입사시켰을 때 내부적으로 한 쌍의 electron-hole pair(EHP)가 여기 되면서 avalanche효과로 전자가 생성되어 내부적으로 증폭되어 단광자를 검출할 수 있다. APD는 그림 1과 같이 Geiger mode로 동작하여 단일광자처럼 미세한 신호를 감지할 수 있다[4]. APD의 breakdown 전압의 1V 이하로 reverse bias를 형성하며 병렬로 4~8V, 4ns의 pulse로 gate를 형성하여 pulse로 감지 윈도우를 만들어 준다.

InGaAs APD의 효율을 최대한으로 하기 위해서는 dark current 노이즈와 after pulse 노이즈를 최소화 하

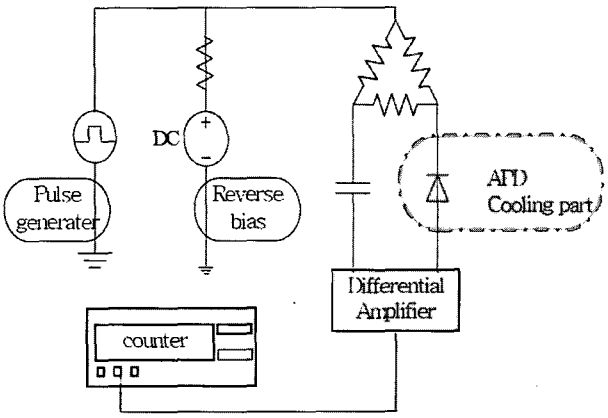


그림 1. 단일광자 감지모듈 회로
Fig. 1. Single photon counting module(SPCM) circuit.

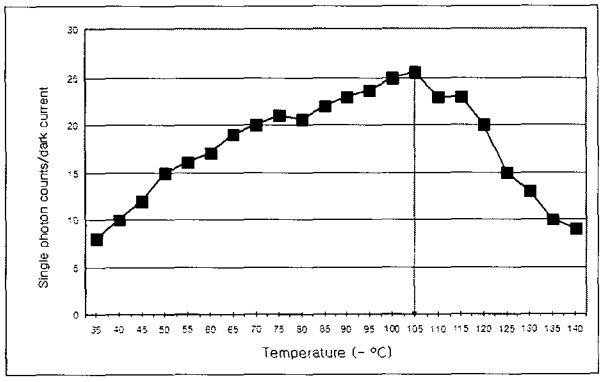


그림 2. 온도별 dark noise당 single photon count
Fig. 2. Single photon counts per dark noise for different temperature.

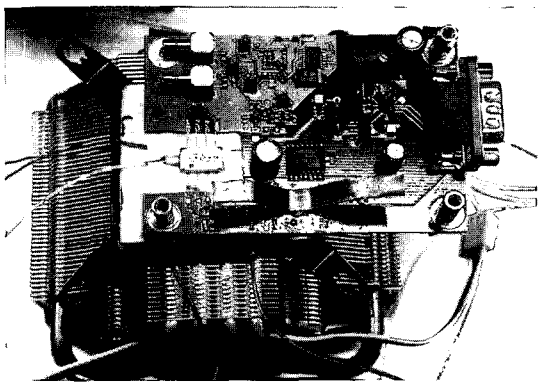


그림 3. 단일광자 감지모듈
Fig. 3. Single photon counting module.

여야 한다. 소자 내에서 열적으로 발생된 전자 정공 쌍에 의해 빛이 없을 때에도 avalanche 효과를 보이는데 이를 dark current라 한다.[5] 그림 2에서 액체질소를 사용하여 냉각시 APD의 노이즈 성분은 선형적으로 감소하여 신호 대 잡음비가 개선되었다. 그러나 그림 2에서와 같이 -105℃ 이하에서 APD 노이즈 성분은 다시 증가하여 신호대 잡음비를 낮추게 되어 결과적으로 APD의 효율은 낮아진다. 이는 after pulse가 원인이며 dark current 성분이 재결합하지 못하고 그 다음 펄스까지 영향을 미치는 것으로 dark current 성분보다 작지만 냉각 될 경우 점점 재결합 확률은 감소하여 노이즈 성분으로 나타나게 된다. 결과적으로는 단일광검출기를 -105℃로 냉각하였을 때, 가장 좋은 효율을 얻을 수 있었다.

위의 결과에서 -105℃에서 가장 좋은 효율을 나타냈지만, Plug & Play 시스템의 집적화를 위하여 TEC와 방열팬, 방열폼 packaging을 사용하였고 이는 -60℃의 냉각 성능을 보여주었다. 또한, Geiger mode circuit을 회로 구성하여 집적화 시킬 수 있도록 PCB로 제작하였다.

제작된 SPCM의 repetition dark count가 식(1)을 통해 확률이 $1x10^{-5}$ 일 경우, quantum efficiency는 식(2)에 의해 15.3%의 효율을 얻었다.

$$dark\ count\ probability = \frac{dark\ frequency}{repetition\ frequency} \quad (1)$$

$$quantum\ efficiency = \frac{signal\ frequency}{\mu \times repetition\ frequency} \quad (2)$$

2. Plug & Play 시스템

Plug & Play 시스템은 자동으로 위상과 편광이 보정

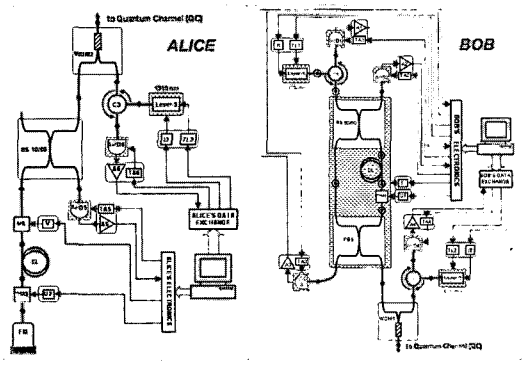


그림 4. Plug & Play가 가능한 양자암호 시스템 구성도
Fig. 4. Schematic of Plug & Play QKD system.

되는 시스템을 말한다. 양자암호시스템 구성 시 plug하기만 하면 faraday mirror(FM)를 이용하여 동일한 경로를 통한 간섭을 이용하므로 위상 및 편광보정이 필요 없어지게 된다. 또한 이를 컨트롤 할 수 있는 컨트롤 보드 또한 개인용 컴퓨터를 USB로 연결 시 자동으로 QKD를 진행 할 수 있도록 광소자들을 컨트롤 할 수 있는 plug & play 시스템을 구성하였다.

Plug and Play 양자암호 시스템의 구성은 그림 4와 같다.

가. 편광 및 위상 보정 시스템

편광 및 위상 보정시스템의 구조는 그림 5와 같다. 강한 세기의 레이저파장(1550nm)은 Bob에서 50/50 beam splitter에 의해 분할된다. 분할된 펄스 중에서 한 펄스는 phase modulator와 delay line을 거치는 긴 경로를 따라가게 되고, 나머지 한 펄스는 짧은 경로를 거쳐 PBS를 통해 광섬유로 전송되며, 이 중 짧은 경로의 펄스는 PBS에서 90도 회전하게 된다. 여기서, Alice와 Bob은 모두 편광이 유지되어야 한다. 두 펄스는 Alice로 들어가게 되며, FM에서 반사되고 PM1에서 0 또는 π, $\frac{\pi}{2}$ 또는 $\frac{3\pi}{2}$ 만큼 Phase shift 된다. Alice를 거쳐 Bob으로 돌아온 펄스는 다시 PBS를 통해 긴 경로와 짧은 경로로 나뉘고 긴 경로의 PM2에서 0 또는 $\frac{\pi}{2}$ 만큼 Phase shift 하여 BS에서 간섭한다. 간섭하는 펄스는 동일한 경로를 지나므로 위상과 편광이 자동적으로 보정된다[6~7]. 마지막으로, 간섭된 신호는 APD1과 Circulator를 지나는 APD2에서 전기 신호로 변환된다.

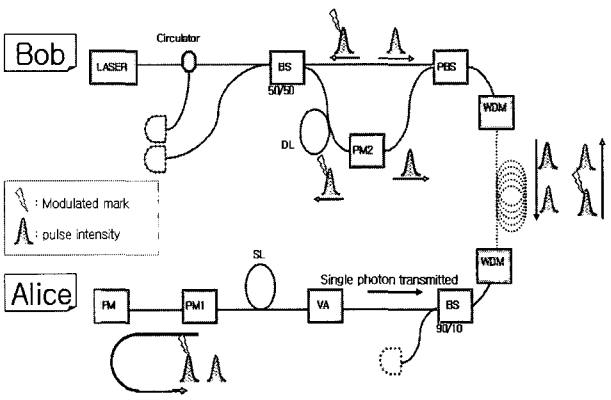


그림 5. 편광 및 위상 보정 시스템
Fig. 5. Phase and polarization auto compensated system.

나. 자동 양자키 분배를 위한 컨트롤 보드

자동 양자키 분배 시스템을 위하여 아래 그림 6와 같이 컨트롤 보드를 구성하였다.

컨트롤 보드는 광학 시스템과 연결되어 모든 QKD 모든 과정을 자동으로 제어하는 기능을 가진다. 시스템 구성은 크게 마이크로컨트롤러와 FPGA 두 가지로 나뉜다. USB 마이크로컨트롤러는 개인용 컴퓨터와 USB 방식으로 연결되며 개인용 컴퓨터에서 개발된 프로그램을 이용해 FPGA 및 주변회로를 제어하고, FPGA와의 데이터교환을 위해 사용된다. FPGA는 주변회로 및 광소자들과 연결된 모든 신호를 제어한다. phase register에는 0, π, $\frac{\pi}{2}$, $\frac{3\pi}{2}$의 디지털 값이 저장되며, D/A 컨버터에서 아날로그 전압값으로 변환되어 그림 7 아래의 Phase modulator driving board를 거쳐 PM을 컨트롤 하게 된다. 여기서 Phase modulator driving board는 정확한 시간에 PM을 제어하기 위한 정확한 아날로그 값을 증폭하기 위해 사용한다. phase register에 저장된

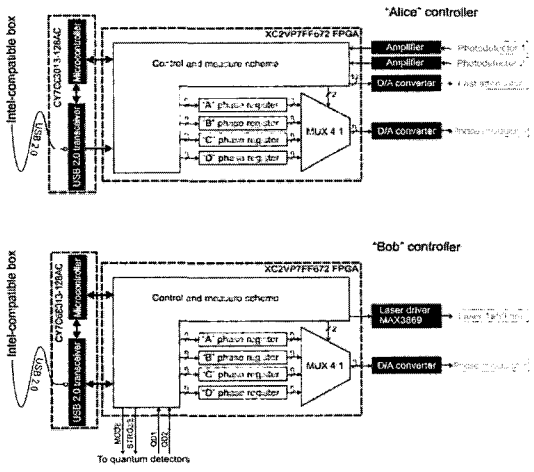


그림 6. Plug & Play 양자암호 시스템을 위한 컨트롤보드 구조도
Fig. 6. Schematic of control board for Plug & Play QKD system.

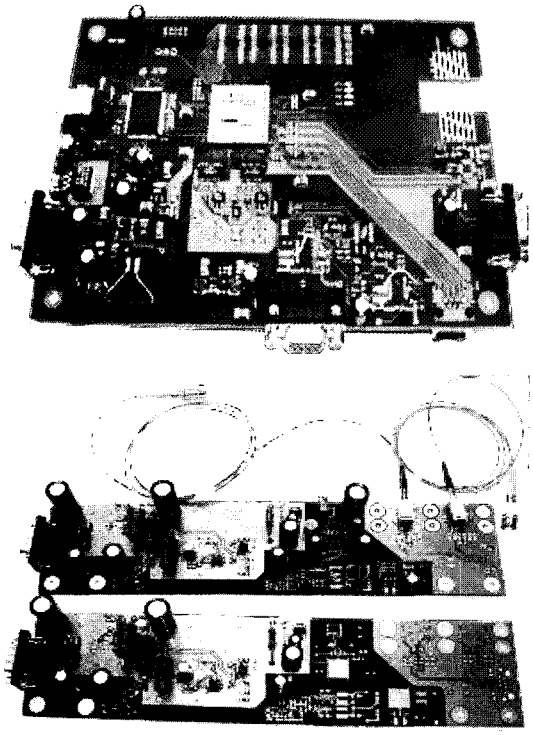


그림 7. Plug & Play 양자암호 컨트롤보드
Fig. 7. Plug & Play QKD control board.

디지털 값이 키의 base가 되며, QKD시 Alice와 Bob의 base를 비교하여 실제 키를 생성하게 된다. Laser 구동은 FPGA에서 나오는 데이터를 laser driver를 사용하여 제어하게 되며 이는 Alice에서 모니터링하여 variable optical attenuator로 단일 광자 광원을 생성하게 된다. SPCM에서 들어오는 신호는 증폭기를 거쳐 FPGA에서 신호 처리한다. 또한, Bob의 FPGA는 단일광자감지기 회로와 연결되어 있어 단일광감지기에서 나온 아주 미약한 신호를 증폭하여 데이터를 구성한다. 위의 모든 과정은 그림 7과 같이 PCB로 집적화된 컨트롤 보드에서 자동으로 수행한다.

Ⅲ. 파라미터 및 전송 결과

전송효율은 양자암호 시스템에서 단일광자의 거리를 제한하는 중요한 파라미터중 하나이다. 전송효율은 다음 식(3)과 같이 나타낼 수 있다.

$$\eta_t = 10^{-\frac{(L_f l + L_B)}{10}} \tag{3}$$

여기서 L_B는 Bob에서의 광학적 손실이고, L_f는 양자채널 손실, l은 전송거리이다.[8]

서로의 base를 비교한 후의 걸러진 양자키 분배율은

표 1. 거리와 펄스당 평균 포톤수에 따른 전송 결과
Table 1. transmission as a result of mean free photon and distance.

channel length		20km	25km	50km	70km	100km
η_t		0.079	0.056	0.01	0.0025	0.0003
R_{sift} (b/s)	μ=0.1	59.25	42	7.5	1.8	-
	μ=0.5	296.2	210	37.5	9.3	1.1
R_{err} (b/s)	μ=0.1	1.98	1.55	0.68	0.54	-
	μ=0.5	7.9	5.75	1.43	0.73	0.52
$QBER$ (%)	μ=0.1	3.2	3.5	8.3	23	-
	μ=0.5	2.5	2.6	3.6	7.2	32

R_{sift}로 나타낼 수 있으며, 이는 식(4)와 같이 나타낼 수 있다.

$$R_{sift} = \frac{1}{2} f_L \mu \eta T \tag{4}$$

여기서 f_L은 거리 L에서의 펄스, μ는 펄스당 평균 포톤수, η은 검출효율, T는 포톤이 analyzer에 도달할 수 있는 가능성이다.

다음으로 중요한 파라미터가 QBER(Quantum Bit Error Rate)이다. 이는 광섬유 내의 안정성과 dark count와 연관이 있으며 양자암호키 분배를 안정적으로 할 수 있는 척도가 된다. QBER은 $\frac{false\,count}{total\,count}$로 나타낼 수 있으며 다음과 같다.

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

여기서 V는 visibility, P_{dark}는 gate 당 dark count 이며, 에러율은 아래식과 같이 구할 수 있다.

$$R_{err} = \frac{1-V}{2} R_{sift} + \frac{1}{2} f_L P_{dark} \tag{6}$$

위 파라미터들을 이용하여, $f_L = 100khz$, $P_{dark} = 1 \cdot 10^{-5}$, $\eta = 15\%$, $V = 0.95$에서 T_{tot}, R_{sift}, R_{err}, $QBER$을 거리L과 μ값을 바꿔가며 실험하였으며 결과는 표 1과 같다.

Ⅳ. 결 론

양자암호 시스템 중 가장 중요한 단일광자감지기의 최적조건에 관한 연구와 자동 QKD 컨트롤러의 개발을 통하여 그림 8의 양자암호 시스템을 완성하였다. 이 시스템은 자동 양자키 분배 방식을 사용하여 25km 거리

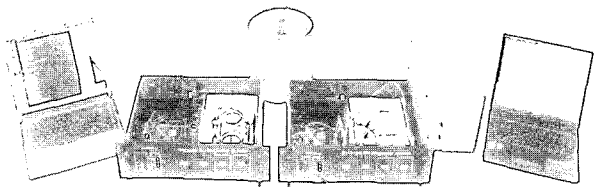


그림 8. Plug & Play 양자암호 시스템
Fig. 8. Plug & Play Quantum cryptography system.

에서 $\mu = 0.1$일 때, $R_{sift} = 42b/s$, $R_{err} = 1.55bps$, QBER = 3.5%를 나타냈다. 양자암호 시스템의 보안성 및 안정성 측면에서 QBER 허용범위가 10~15%까지라고 할 때[9], $\mu = 0.1$ 일때 50km 이상의 전송거리를 확보하였고, 이는 시스템화 및 모듈화 할 수 있는 컨트롤 보드와 함께 상용화가 가능한 수치이다.

참 고 문 헌

[1] C. H. Bennett and G. Brassard, in proceedings of the international conference on computer systems and signal processing, Bangalore, IEEE, New York, pp. 175-179, 1984.

[2] C. H. Bennett and F. Bessette, J. Cryptol. 5, 3 (1992).

[3] Muller A, Herzog T, Huttner B, Tittel W, Zbinden H and Gisin N , "Plug&play systems for quantum cryptography," *Appl. Phys. Lett.* 70 793 - 5, 1997.

[4] P. C. M Owens, J. G. Rarity, P. R. Tapster, D. Knight, P. D . Townsend, "Photon counting with passively quenched germanium avalanche," *Appl. Opt.* 33, p.6895 1994.

[5] Stucki D, Ribordy G, Stefanov A, Zbinden H, Rarity J G and Wall T "Photon counting for quantum key distribution with Peltier cooled InGaAs APDs" *J. Mod. Opt.* 48 1967 - 82, 2001.

[6] Ribordy G, Gautier J-D, Gisin N, Guinnard O and Zbinden H "Fast and user-friendly quantum key distribution" *J. Mod. Opt.* 47 517 - 31, 2000.

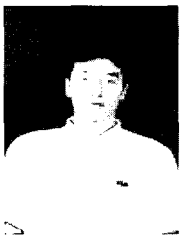
[7] Bethune D and Risk W "An auto-compensating fiber-optic quantum cryptography system based on polarization splitting of light," *IEEE J. Quantum Electron.* 36 340 - 7, 2000.

[8] N. Namekata, Y. Makino, ans S. Inoue, "Single-photon detector for long-distance fiber-optic quantum key ditribution," *Opt. Lett* 27, p.954, 2002.

[9] J. Kim, O. Benson, H. Kan, and Y. Yamamoto, "A single-photon Turnstile device," *Nature,* Vol.397, p.500, 1999.

저 자 소 개

이 경 운
2006년 세종대학교 전자공학과 학사졸업.
2006년~현재 고려대학교 전자전기공학과 석사과정.
<주관심분야 : 양자암호, 볼로미터,DSP>

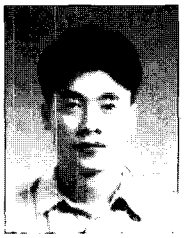


박 준 범
2005년 세종대학교 전자공학과 학사졸업.
2007년 연세대학교 전자공학과 석사졸업.
2007년~현재 UST 전자공학과 박사과정.
<주관심분야 : 양자암호, 볼로미터,DSP>

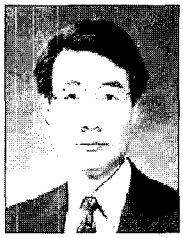
신 현 준
1995년 KAIST 물리과 석사졸업.
2000년 KAIST 물리과 박사졸업.
2006년 현재 KIST 선임연구원
<주관심분야 : 나노바이오센서, 양자암호>

문 성 욱
1988년 연세대학교 금속공학과 석사졸업.
1994년 연세대학교 반도체공학과 박사졸업.
2006년 현재 KIST 나노바이오 연구센터 센터장
<주관심분야 : 나노바이오센서, 양자암호, 볼로미터>

박 철 우
2005년 세종대학교 전자공학과 학사 졸업.
2007년 연세대학교 전자공학과 석사 졸업.
KIST 학생연구원
<주관심분야 : 양자암호, 마이크로센서.>



이 승 훈
2001년 울산대학교 기계공학과 석사 졸업.
2004년~현재 서울대학교 기계항공공학부 박사과정
<주관심분야 : 마이크로/나노센서, 엑츄에이터>



박 정 호
1981년 고려대학교 전자공학과 학사 졸업.
1987년 University of Delaware 전자공학과 박사 졸업.
1990년~현재 고려대학교 전자전파공학부 교수
<주관심분야 : 광소자분야, 전자소자 분야>