1 550nm 파장대역의 량자암호열쇠분배 조종장치설계의 한가지 방법

한광복, 김춘근

경애하는 **김정은**동지께서는 다음과 같이 말씀하시였다.

《통신망의 보안능력을 결정적으로 높여야 합니다.》

오늘날 정보의 안전성은 매우 중요한 문제로 제기되고있으며 안전한 정보교환을 어떻게 보장하는가 하는것이 절박한 과제의 하나로 되고있다.

현재 암호통신분야에서 세계적으로 량자물리학의 기본원리에 기초한 암호기술 즉 량자암호통신기술이 큰 주목을 끌고있다.[3, 4]

지난 시기 개발한 량자암호통신기는 850nm 파장대역의 빛섬유를 리용하여 암호열쇠분배를 실현한것으로 하여 현재 광범히 쓰이는 1 550nm 파장대역의 빛섬유에서는 리용할수 없다.

론문에서는 1 550nm 파장대역에서 량자암호열쇠분배를 위한 조종장치설계의 한가지 방법을 제안하고 실험을 통하여 그 성능을 확증하였다.

1. 송신기조종장치의 설계

BB84규약에 기초한 량자암호통신에서는 4개의 빛량자상태가 리용되며 따라서 4개의 반도체레이자2극소자가 리용된다.[2]

일반적으로 BB84규약[1]에서는 전기적임풀스에 의해 해당 반도체레이자를 구동하고 광학적으로 그것의 세기를 감쇠시켜 평균빛량자수를 0.1로 보장한다.

한편 반도체레이자2극소자에서 발생하는 레이자빛의 세기는 턱전류를 초과할 때 급격히 증가한다.

따라서 반도체레이자2극소자를 빠른 속도로 구동시키려면 일정한 편의전류를 가해주고 여기에 변조임풀스를 가해주어야 한다.

그래야 반도체레이자2극소자에 흐르는 전류가 턱전류이상으로 되면서 빛방출량이 급격히 증가한다.

론문에서 제안한 송신기조종장치는 콤퓨터와의 자료통신을 위한 한소편처리기(ARM)와 레이자구동조종을 위한 FPGA, 토대렬을 기억시키기 위한 RAM, 반도체레이자들과 그 구동회로들로 구성되여있다. 여기서 토대렬은 BB84규약에 기초한 량자암호열쇠렬을 의미한다.

콤퓨터로부터 생성된 토대렬은 RAM에 기억되며 FPGA는 1MHz의 주파수로 토대를 읽고 동기신호와 함께 해당한 레이자를 구동시킨다.

그림 1과 2에 송신기조종장치구성도와 송신기조종알고리듬을 보여주었다. 그림 2에서 QKD는 량자암호열쇠분배(Quantum Key Distribution)의 략어이다.

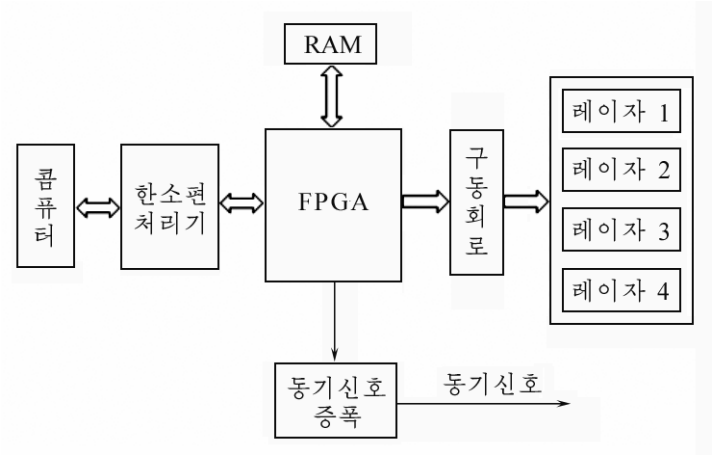

그림 1. 송신기조종장치구성도

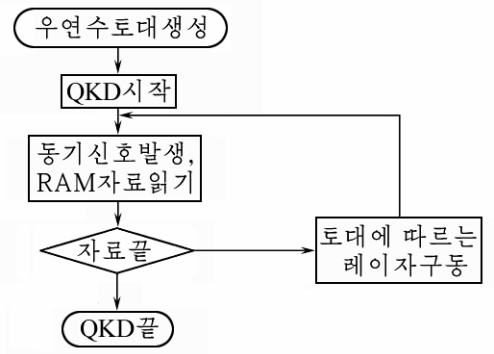

그림 2. 송신기조종알고리듬

2. 수신기조종장치의 설계

송신기에서 발생된 매개 상태의 빛량자신호는 동기신호에 따라 수신기에로 전달된다.

빛의 전달통로가 고정되여있는 조건에서 매질속에서의 빛의 전달속도를 고려하면 빛량자가 단일빛량자검출기에 도착하는 시간을 계산할수 있다.

이로부터 단일빛량자검출기를 해당한 빛량자가 도착하는 시간대역에서 동작시키면 높은 정확도로 빛량자를 검출할수 있다. 즉 빛섬유와 편극빛분할기를 리용하여 동기신호에 대하여 빛량자의 도착시간을 통로별로 지연시키면 4가지 편극상태를 가지는 빛량자들을 1개의 단일빛량자검출기로 측정할수 있다.

단일모드빛섬유(중심파장 1 550nm, 모드마당직경 5.6μm, 감쇠률 2dB/km)에서 빛이 전파할 때 그것의 지연시간은 대략 5ns/m(t_d)이다.

량자통신로의 빛섬유의 길이를 L, 수신기에서 i번째 통로의 건늠선의 길이를 L_i, 기타 빛섬유광학요소의 길이를 L_0 (11m)이라고 하면 반도체레이자2극소자로부터 빛량자검출기까지의 i번째 통로에서의 지연시간(T_i)은 다음과 같다.

$$T_i = t_d \times (L + L_i + L_0)$$

한편 동기신호의 전파속도는 빛속도 c와 같으므로 량자통신로의 길이와 동기신호선로의 길이가 같다고 하면 동기신호의 지연시간(T_d)은 다음과 같다.

$$T_d = L/c$$

따라서 i번째 빛량자의 상태를 측정하기 위하여 빛량자검출기에 가해주는 문조종신호의 지연시간 t_i는 동기신호가 검출된 시각으로부터 다음과 같다.

$$t_i = T_i - T_d$$

1개의 빛량자검출기를 리용한 빛량자상태의 측정방법에서는 매개 상태의 빛량자가 통과하는 전체 통로의 길이가 주어진 조건에서 송신되여오는 빛량자상태신호를 시분할하여 측정을 진행한다.

그림 3에 수신기조종장치구성도를 보여주었다.

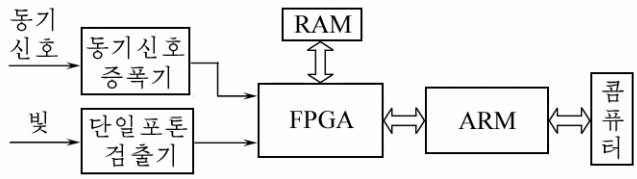

그림 3. 수신기조종장치구성도

그림 3의 RAM에는 토대렬에 기초하여 생성된 4bit의 우연자료가 기억되여있다. 이 우연자료들은 동기신호에 따라 4bit단위로 FPGA를 통하여 단일빛량자검출기에 문조종신호로 가해진다. 그리고 량자통신로로부터 들어온 빛량자신호는 문조종신호에 의하여 조종되는 단일빛량자검출기에서 전기적임풀스로 변환된다.

FPGA에서는 동기신호와 문조종신호에 기초하여 입력되는 단일빛량자검출기의 출력임풀스의 상태를 측정하고 결과를 RAM에 기억시킨다.

수신기조종알고리듬을 그림 4에 보여주었다.

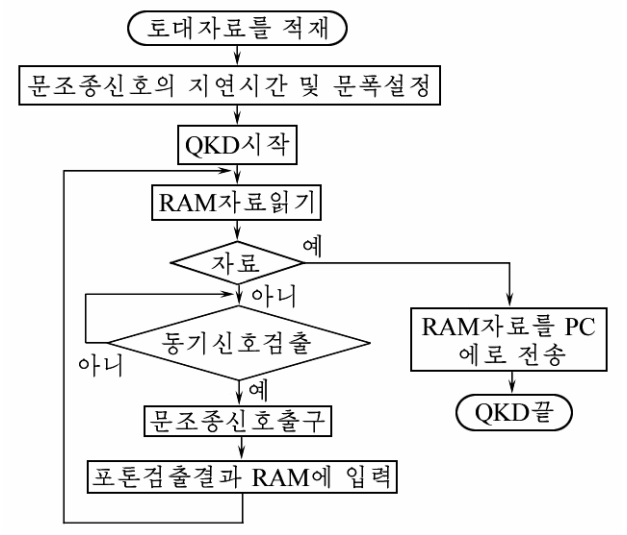

그림 4. 수신기조종알고리듬

3. 통신실험 및 결과분석

론문에서 제안한 설계방법에 기초하여 량자암호통신기를 제작하고 음성과 화상에 대한 통신실험을 진행하였으며 그 성능을 이전의 850nm 파장대역의 량자암호통신기와 비교하였다. 그 비교결과를 표에 보여주었다.

표. 비교결과

지표	단위	선행한 방법[1]	제안한 방법
레이자빛파장	nm	850	1 550
조종단읽기, 쓰기속도	kbps	256	2 560
열쇠생성속도	kbps	8.86	80
오유수정후오유률	%	10^{-2}	10^{-3}
처리소자		FPGA	FPGA, ARM

표를 통하여 제안한 방법에 기초한 조종장치가 이전의 조종장치에 비하여 열쇠생성속도는 대략 9배 증가하였다는것을 알수 있다. 여기로부터 1 550nm 파장대역의 빛섬유를 리용하여 량자암호통신을 실현할수 있다는것을 확증하였다.

맺 는 말

1 550nm파장대역에서의 량자암호열쇠분배를 위한 한가지 조종장치설계방법을 제안하고 실험을 통하여 제안한 방법이 선행한 방법에 비하여 성능이 훨씬 개선되였다는것을 확증하였다.

참 고 문 헌

[1] **김일성**종합대학학보(자연과학), 50, 1, 57, 주체93(2004).

[2] 김남철; 량자정보물리, **김일성**종합대학출판사, 280～286, 344, 주체103(2014).

[3] P. Kok et al.; Rev. Mod. Phys., 79, 135, 2007.

[4] M. T. Cheng et al.; Phys. Rev., 85, 053840, 2012.

주체110(2021)년 2월 5일 원고접수

A Design of Quantum Key Distribution Control Device for 1 550nm Wavelength Band

Han Kwang Bok, Kim Chun Gun

We proposed a design of control device for quantum key distribution in 1 550nm wavelength band and made the experiment. As a result, we confirm that the control device based on the proposed design improves in performance than previous one.

Keywords: quantum key distribution, BB84 protocol, single photon detector