양자암호화 키 전송에서 검출기 특성에 따른 전송효율

조기현 · 강장원 · 윤선현†

전남대학교 자연과학대학 물리학과

㉾ 500-757 광주광역시 북구 용봉동 300번지

(2000년 11월 1일 받음, 2001년 3월 20일 수정본 받음)

자연의 법칙이 보장해 주는 완벽한 보안이 가능한 양자암호화 통신을 위해서는 아주 약한 빛을 사용해 한 펄스에서 두 개 이상의 광자가 발견될 확률을 아주 작게 해야한다. 그러나 잡음과 검출기의 양자효율 등을 고려하면 현실적으로는 실험적 상황에서 발생되는 신호왜곡과 도청에 의한 신호왜곡을 구별해 낼 수 있는 조건을 찾아내야 한다. 검출기에 걸어주는 전압의 크기와 신호검출시의 문턱전압을 변화시켜가며 여러 세기의 빛에 대한 양자암호화 키 전송가능성을 실험적으로 확인하였다. 암호화 키 전송 방식은 잘 알려진 두 가지 선형편광과 두 가지 원형편광 상태를 이용한 4-state 암호화 키 전송방식을 사용하였다.

분류코드 : QO.010, QS.010

I. 서 론

빛을 통신에 응용하면서 단위 시간당 전송되는 정보의 양은 급속도로 증가하고 있고 더 많은 양의 정보를 효과적으로 빨리 보내고 처리하는 기술력의 확보가 정보화 산업의 핵심 분야가 되었다. 그런데 많은 노력들이 대용량의 정보를 빠르게 보내는데 주력하고 있을 뿐 안전하게 보내는데는 상대적으로 노력이 부족한 편이다. 보안이 필요한 정보는 운송하는 과정에서 도청되어 질 수 있고 도청 당한 정보는 정보로서 의미를 상실했는데도 주고받는 사람은 그 사실조차도 모를 수 있다.

정보보호를 위해 지금까지 사용된 고전적인 암호화 방법은 여러 방법들이 있으나 대표적인 것들은 DES(Date Encryption Standard)방법, RSA(Rivest-Shamir Adleman)방법, 그리고 Knapsack ciphers 등이 있다.[1] 이와 같은 고전적 방식의 암호화는 엄밀히 말하여 완벽한 안전을 보장하는 것이 아니라 현실적으로 풀기 어렵다는 조건부 안전에 의존하고 있다. 따라서 만약 도청자가 좋은 알고리즘이나 충분한 시간을 갖는다면 정보저장에 많이 사용되는 DES와 통신에서 널리 사용되는 RSA까지도 원칙적으로 해독될 수 있다.

가장 성공적인 고전적 암호화 통신 방법중 하나인 RSA방법의 안전성은 큰 수를 소인수 분해하기가 어렵다는 사실에 의존하고 있다. 소인수 분해는 기존의 컴퓨터가 하기 힘든 일중의 하나로 숫자 n을 소인수 분해하기 위해서는 지금까지 알려진 고전적 방법으로는 대략 $\exp(\sqrt{\log n \log(\log n)})$번의 연산이 필요하다.[2] 그러나 근래에 개발된 Shor의 양자 소인수 알고리즘은 고전적인 방법으로 불가능해 보였던 664비트 정도의 큰 수를 수초이내에 소인수 분해할 수 있는 방법을 보여준다.[3] Shor의 양자알고리즘을 위해 필요한 양자계산기의 기본이 되는 양자비트도 최근에 여러 방법으로 개발되어지고 있다.[4-6] 이와 같이 발달하는 기술과 이론은 고전적인 암호화 통신이 더 이상 안전할 수 없음을 예견하고 있다.

따라서 이러한 방법론이나 기술의 발달에도 암호를 풀 수 없는 새로운 방법이 요구되어졌고 이러한 목적을 위해 빛의 양자역학적 특성을 이용한 양자 암호화 방법이 연구되어 왔다.[7-10]

양자암호화 방식은 임의의 양자적 상태를 복사할 수 없다는 자연법칙이 안전성을 보장해 주는 방법으로 구체적으로는 하나의 광자의 4가지 서로 다른 편광상태[7]를 이용하거나 Poldowski-Rosen 엉킴 쌍,[8] 두 가지 비직교상태,[9] 그리고 편광상태가 아닌 위상변조를 이용하는 방법 등[10] 여러 가지가 있다.

위에 언급한 방법들은 성공적으로 도청 사실을 알 수 있으며 이렇게 하기 위해서는 하나의 광자 펄스를 보내야 한다. 만약 송신자가 보낸 빛이 둘 이상이면 이 빛을 도청자가 뽑아내어 나눈 다음 각각에서 키에 관한 정보를 얻어내면 송신자가 보낸 키에 관한 정보를 완벽하게 알아 낼 가능성이 생기기 때문이다. 따라서 도청자는 키에 관한 정보를 도청한 다음에 그 키의 관한 정보를 이용해 수신자에게 보내면 송신자와 수신자는 키의 관한 정보가 도청된 지 모르게 되어 암호화 통신이 불가능해 진다. 따라서 빛을 하나씩 보내야 하나 지금까지의 기술로는 한 개씩 보내기는 어려워 아주 약한 상태의 빛을 보내 신호에서 광자를 두 개 이상 발견할 확률을 아주 작은 값이 되게 하는 수밖에 없다. 그런데 이 경우 빛이 진행하면서 생기는 손실과 측정과정에서 생기는 손실 등이 도청 때문에 유입되는 신호왜곡보다 더 적게 만드는 일이 필요하다.

본 연구는 빛의 세기가 이런 현실적 문제가 포함된 양자 암호화 통신의 실현 가능성을 구체적 실험 환경 내에서 밝힌다. 먼저 4-state를 이용한 암호화 통신을 간략하게 설명하고 또 암호화를 하기 위해서는 약한 빛을 이용해야만 하는 이유를 실험적으로 보여 이것을 구현할 때 여러 실험 조건에 따라 암호화 통신이 가능한 조건을 찾았다. 원칙적으로는 보내는 빛을 한번에 광자 한 개씩 보내고 검출기는 양자 효율이 1 인 측정기로 잡음 없이 측정하면 되나 실제상황에서는 이런 조건이 만족되지 못하므로 적절한 조건을 찾아내야 한다. 조건을

†E-mail : sunyoun@chonnam.ac.kr

찾기 위해서는 주어진 실험실 상황에서 변화시킬 수 있는 변수인 신호의 크기, 검출기의 이득, 측정된 신호의 0과 1을 결정짓는 문턱전압 등을 변화시켰다.

II. 4-state 암호화방법

BB84[11]로 알려진 4-state를 이용한 양자암호화 통신은 송신자가 단위 시간당 한 개의 광자를 보내면서 편광의 방향을 선형이나 원형편광을 만들어 각각 두 가지 가능한 성분중 한가지 방법을 임의로 택해 보낸다. 이것은 송신자가 편광방향을 네 가지 중 임의의 하나를 보내는 것을 의미한다. 수신자는 검출기를 선형 또는 원형편광된 빛을 측정할 수 있도록 임의로 조정해 가면서 광자를 검출한다. 그런 다음 대외적으로 각 광자에 대하여 측정결과가 아닌 자기가 사용한 편광방향이 선형인지 원형인지를 서로 밝혀 이중 같은 방법을 택하였고 성공적으로 측정된 정보를 사용하여 암호화 키를 만든다. 만약 누군가 신호를 도청했다면 암호화 키로 사용하기로 한 자료중 임의로 일부를 선택하여 송신자와 서로 비교해 보면 일치하지 않은 부분이 기준치 이상이 된다. 그럴 경우 그 키는 도청되었으므로 버리고 다른 채널을 이용하여 다시 키를 송수신한다.

본 실험에서 사용한 구체적인 방법은 송신자가 선평편광된 약한 펄스의 빛의 위상을 전기광학변조기(Electro-Optic Modulator)로 임의로 변조시킨다. 초기 빛의 편광을 나타내는 존스행렬

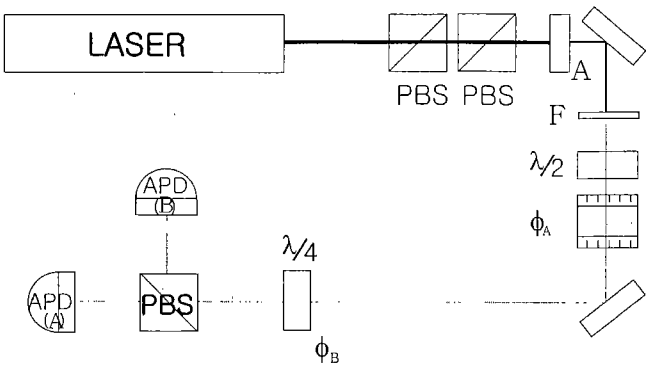

그림 1. 양자 암호화를 위한 실험 장치 배열이다. PBS: 편광분할장치, A: attenuator, F: 필터, APD: Avalanche Photodiode, $\frac{\lambda}{2}$: 위상지연판.

(Jones matrix)이 $\begin{pmatrix}1\\1\end{pmatrix}$이 되게 선형편광시킨다. 그런 다음 변조기로 새로운 위상지연(ϕ)를 0, 90, 180, 270로 변화시키면 송신기 출력단에서 출력된 빛의 편광상태는 다음식

$$\begin{pmatrix}1 & 0\\ 0 & E^{-i\psi}\end{pmatrix}\begin{pmatrix}1\\1\end{pmatrix} \tag{1}$$

에 따라서 편광상태가 $\begin{pmatrix}1\\1\end{pmatrix},\begin{pmatrix}1\\-i\end{pmatrix},\begin{pmatrix}1\\-1\end{pmatrix},\begin{pmatrix}1\\i\end{pmatrix}$이 된다. 따라서 송신자는 전기광학변조기의 전압을 조절하여 45 선형편광, 우향원편광, –45 선형편광, 좌향원편광을 만들 수 있다.

수신자 역시 그림 1에서와 같이 다른 전기광학변조기로 전송된 빛의 위상을 조절 할 수 있다. 수신자는 검출기 B에 45도의 선형 편광빛이 도달하고 검출기 A에는 –45도의 선형 편광빛이 도달하도록 편광분할기를 놓는다. 만약 수신자가 도달한 빛에 위상지연을 0°더하면, 전송된 빛의 편광은 변화되지 않으므로 수신자가 검출기 B(A)에서 광자를 검출했다면 송신자가 45°(–45°)의 선형 편광된 빛을 보냈다고 결론 내릴 수 있다. 만약 송신자가 좌, 우원형 편광에 관계없이 원형 편광된 빛을 보냈다면 각각의 검출기에서 발견될 확률은 두 경우 모두 50%이다. 그러므로, 수신자가 0° 위상지연을 줄 경우 송신자가 보낸 편광이 선형 편광인 경우일 때의 결과만을 양자키로 사용될 수 있다. 만약 수신자가 90° 위상지연을 더하면 송신자가 보낸 45°선형, 우향 원형, –45°선형, 좌향 원형은 변조기를 지난 후 각각

$$\begin{pmatrix}1\\1\end{pmatrix},\begin{pmatrix}1\\-i\end{pmatrix},\begin{pmatrix}1\\-1\end{pmatrix},\begin{pmatrix}1\\i\end{pmatrix} \tag{2}$$

로 변화된다. 즉 수신자는 우향 원형, –45°선형, 좌향 원형, 45° 선형이 된다. 이 때 수신자가 검출기 B(A)에서 광자를 검출한 확률은 우(좌)원형 편광된 빛에 대해서는 각각 1이다. 만약 송신자가 보낸 빛이 선형편광된 빛이었다면 45°나 –45°선형, 편광에 관계없이 두 검출기에서 각각 50%의 확률로 관측된다. 표 1에는 여러 경우에 대한 예가 나타나 있다.

양자암호화 통신을 하기 위해서 송신자는 네 개의 양자상태 중 매번 임의로 한 상태를 선택하여 펄스를 보내고, 수신자는 매번 임의로 원형이나 선형으로 측정 장치를 설치하여 검출기 A의 결과를 기록한다. 표 1에서 2, 3, 5, 6, 7, 10인 경우들은 송신자와 수신자가 원형 또는 선형 편광인 빛의 상태를 검출하기 위한 장치를 같이 사용하였기 때문에 수신자는 측정

표 1. 약한 빛에 대한 가능한 실험 데이터 (◎ 원형편광 측정장치, ×선형편광 측정장치)

		1	2	3	4	5	6	7	8	9	10
송신자	좌표계	◎	×	◎	◎	×	◎	×	×	◎	×
	위상지연	90	0	90	270	180	270	0	180	270	0
	편광상태	R	↗	R	L	↖	L	↗	↖	L	↗
수신자	좌표계	×	×	◎	×	×	◎	◎	◎	×	×
	위상지연	0	180	90	180	0	90	90	90	180	0
	편광상태	R	↖	↖	R	↗	↗	R	L	R	↗
검출기	a(↖)	(1,0)	1	1	(1,0)	0	0	(1,0)	(1,0)	(1,0)	0
	b(↗)	(1,0)	0	0	(1,0)	1	1	(1,0)	(1,0)	(1,0)	1
Key (?)		NO	OK	OK	NO	OK	OK	NO	NO	NO	OK

결과로부터 송신자가 어떤 편광 상태의 빛을 보냈는지를 정확하게 알 수 있다. 반면에 1번의 경우 수신자가 검출기 A에서 비록 광자를 측정하였다 하더라도 이 광자가 우선형 편광인지, 좌 선형편광인지를 구별할 수 없기 때문에 정보로서의 의미를 상실한다. 따라서 검출 후 서로 사용한 검출장치를 공개적으로 밝혀 같은 검출장치를 사용한 경우만의 측정치를 자료로 사용하면 원하는 양자암호화 키를 만들 수 있다.

다음으로 누군가 도청을 하게 되면 신호가 어떻게 바뀌는지를 보자. 보내는 빛이 광자 한 개일 경우 도청자는 빛을 가로채어 그 일부만을 측정할 수 는 없고 완벽한 복사도 불가능하다.[12,13] 도청이 성공하기 위해서는 광자 한 개를 측정하여 그 결과로부터 원래의 상태를 예측하고 그 정보를 입수한 후에 송신자에게 같은 신호를 보내주어 송신자가 도청한 사실을 알아내지 못하게 해야한다. 한 예로 송신자가 보내는 빛이 우원형편광이고 수신자가 원형편광 상태를 검출하도록 검출기를 조정하였다면 수신자는 정확하게 송신자가 우원형편광빛을 보낸 것을 알 수 있다. 그런데 이 때 만약 누군가 도청을 하여 이 정보를 얻어내려면 도청하는 사람은 송신자가 보낸 빛이 원형편광인지 선형편광인지를 알 수 없기 때문에 검출장치를 임의로 둘 중 하나에 맞추어야 한다. 50%의 확률로 원형편광 상태를 예측할 수 있고 이 경우 도청한 빛이 우원형편광이라는 사실을 알아낸 후 수신자에게 우원형편광된 빛을 다시 보낼 수 있어 성공적인 도청이 가능하다. 그러나 다른 50%의 확률로 선형편광상태를 예측하여 측정하면 결과는 45°나 –45° 선형편광된 빛을 송신자가 보냈다는 결과를 얻게 되어 이 정보를 확인한 후에 수신자에게 확인된 정보 즉 45°나 –45선형편광된 빛을 보내게 되면 수신자가 송신자와 같은 편광상태를 측정할 장치를 꾸몄음에도 불구하고 25% 확률로 잘못된 결과를 얻게된다. 따라서 누군가 도청하였을 경우 수신자와 송신자가 같은 편광검출상태를 만들어 암호화 키로 사용하려 했던 자료 중 일부를 공개해 비교해 보면 25% 정도의 키가 차이를 보이게 된다. 결론적으로 같은 장치 내에서 확이한 자료가 차이를 보여주면 누군가 도청을 했다고 결론 지을 수 있고 그렇지 않은 경우에는 안전하다고 결론지을 수 있다.

III. 실 험

양자 암호화 통신을 하기 위해서는 아주 약한 세기의 빛을 이용해야 한다는 것을 알고 있다. 그러나 현실적 조건에서 암호화 키를 안전하게 보낼 수 있는 영역을 찾아내기 위해 기존의 장치들을 사용하여 그림 1과 같은 실험 장치를 꾸몄다. 기존의 광학 부품들과 장치들의 성능을 고려하여 광원은 Q-Switched(반복율 1 KHz) Nd:YAG 레이저를 사용하였는데 빛의 세기가 아주 약한 상태를 만들 땐 편광분할기와 필터등을 사용하였다.

본 실험에서 사용된 검출기는 Newport사 877 Avalanche photodiode이며 검출기에 입사된 빛은 오실로스코프에서 펄스 형태로 측정하였다. 송신자는 선형편광된 빛을 전기광학변조기를 통해 임의로 위상지연(ψ_A)을 시킨다. 이 때 변조시킨 빛은 위상지연에 의하여 4개의 편광상태를 만들 수 있다. 이렇게 보내진 빛은 송신기로 부터 1.5 m 떨어진 수신기에 도달한 후 위상지연판(ψ_A)에 의해 위상지연 되어 편광분할기를 통하여 검출된다. 우리는 먼저 약한 세기의 빛과 강한 세기의 빛을 측정하였다. 이때 사용된 강한 빛의 세기의 평균 광자수는 5×10^{12}개이며, 약한 빛의 세기의 평균 광자수는 대략 10개 이하이지만 실제 측정에서 관측된 결과만 고려하였다.

송신자는 빛을 임으로 편광 시켜 보내고 수신자는 0와 90로 위상지연을 시켜 두 결과를 비교하였다. 수신자가 두 검출기 A, B에서 광자를 검출할 확률이 50%이며 만약 송신자가 하나의 광자를 보낸다면 두 검출기 A, B에서 동시에 광자를 발견하는 것은 불가능하다. 그림 2에서 보여진 데이터 a_1, b_1은 강한 세기의 빛에 대하여 한번 측정한 값이고 그 값에 대한 평균값은 A, B이다. 강한 빛에 대한 그림 2(b)의 데이터는 적

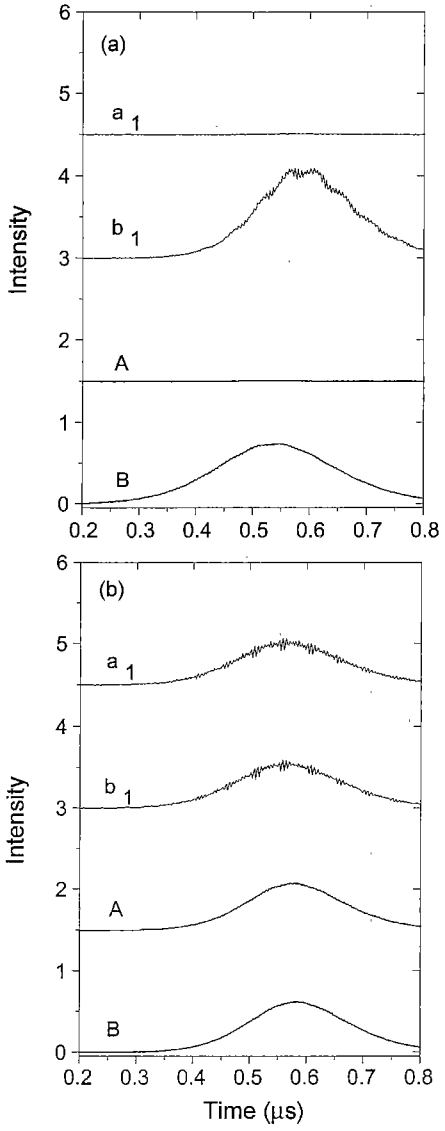

그림 2. 필터를 제외 시킨 상태에서 송신자는 45 선형편광된 빛을 보내고 수신자는 (a) $\psi_b = 0$ (b) $\psi_b = \frac{\pi}{2}$ 위상지연 시켜 두 검출기에서 검출하였다. 빛의 세기는 동일 하며 편의상 1.5이동하여 나타냄.

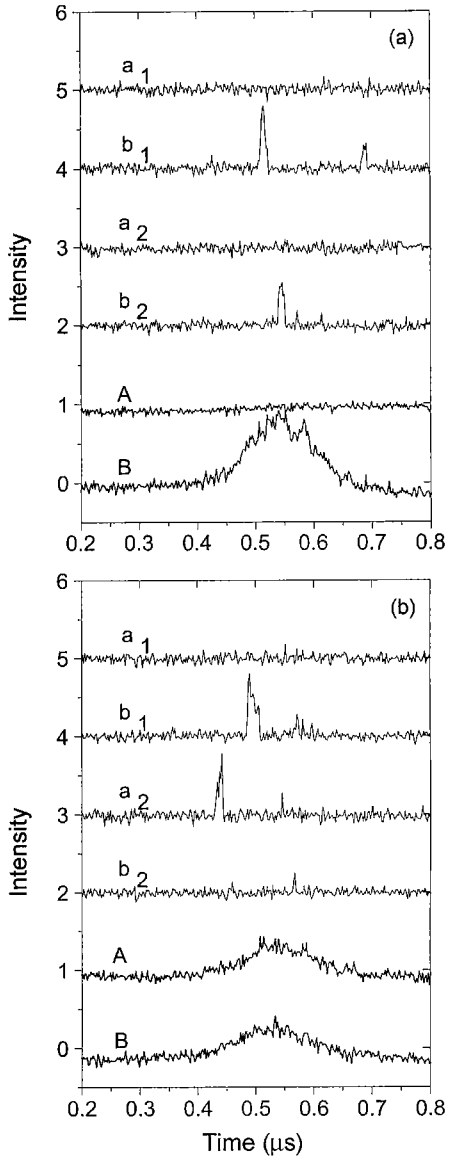

그림 3. 필터를 포함 시킨 상태에서 송신자는 45 선형편광된 빛을 보내고 수신자는 (a) $\psi_b = 0$ (b) $\psi_b = \frac{\pi}{2}$ 위상지연 시켜 두 검출기에서 검출하였다. 여기에서 사용된 필터는 빛의 세기를 입사광에 대하여 1/50000로 감쇠시킨다. 빛의 세기는 동일하며 편의상 1이동하여 나타냄.

어도 두 개 이상의 광자가 있다는 것을 보여주고 있다. 위의 실험적 결과를 표 1과 비교한다면, 그림 2(a)는 표 1에서의 10번째를 나타내는 것이며 그림 2(b)는 표 1에서의 7번째를 나타낸 것이다.

다음은 약한 빛에 대하여 위 실험장치와 동일한 측정을 하였다. 그림 2(b)와 그림 3(b)를 비교하면 이 둘 사이에 큰 차이가 있음을 알 수가 있다. 그림 2(b)에서 보여진 데이터는 한번 측정한 값 a_1, b_1과 그 평균값 A, B가 동일한 그래프로 나타났지만 그림 3(b)의 데이터(a_1, b_1, a_2, b_2)와 그 평균값 A, B는 다르다. 그림 3(b)의 평균값 A, B와 그림 2(b)의 평균값 A, B가 정량적으로는 동일한 값을 갖는다. 그러나 한 번 측정한 펄스데이터는 그림 3(b)에서 존재하지만 그림 2(b)에서는 존재하지 않는다. 따라서 우리는 검출기 $B(b_2)$에서 광자를 발견할 수가 없지만 검출기 $B(b_1)$에서 광자가 발견된다는 것을 알 수 있다. 검출기 A와 B에서 광자를 검출할 수 있는 확률이 항상 50%로 동일할지라도 각각의 검출기에서 동시에 광자를 볼 수 있는 데이터는 없다. 그러므로 이러한 사실들로부터 양자 암호화 통신을 하기 위해서는 약한 펄스를 이용해야 한다는 것을 알 수 있다. 더구나 이런 경우 도청자가 정보를 도청하더라도 수신자와 송신자는 도청된 사실을 알 수가 있다.

우리는 양자암호화 통신을 하기 위해 약한 세기의 빛을 검출하였다. 그러나 검출 시 하나의 펄스 안에 하나의 광자가 검출된다는 것을 확신할 수가 없다. 그래서 우리는 양자효율이 1이 아닌 검출기의 현실적인 문제들을 고려했을 때 실현 가능한 영역을 찾아보았다. 송신자는 임의의 편광 중 하나를 임의로 보내고 수신자는 편광된 빛을 λ/4로 위상지연을 시켜 검출하였다. 검출기는 약한 세기의 빛을 검출하므로 좋은 이득과 반응성능을 얻을 수 없었다. 그래서 인가전압을 걸어주어 검출기의 이득과 반응성능을 향상시켜 양자효율을 최적화 시켰다. 그러나 검출기의 반응성능은 빛에 의한 신호 뿐 아니라 잡음에 대해서도 향상시켜 주었기 때문에 오실로스코프의 문턱전압을 조절하여 문턱전압의 이상이 올 때 빛에 의한 신호로 받아들이고 이하는 잡음에 의한 신호로 생각하였다.

먼저 검출기의 인가전압과 오실로스코프의 문턱전압을 조절하여 빛의 세기에 따른 SNR를 크게 할 수 있는 인가전압을 알아보았다. 그림 4는 인가전압이 91.4 V일 때 빛의 세기와 문턱전압의 관계를 나타낸 것이다. 인가전압이 너무 낮을 때와 높을 때는 문턱전압에 관계없이 SNR이 아주 낮았지만 91.4 V에서는 빛의 세기와 문턱전압에 따라 신호와 잡음을 확실히 구별할 수 있었다. 문턱전압이 0.5 mV 이하인 영역에서는 신호인 경우의 펄스와 잡음에 의한 펄스에 대하여 발견될 확률이 1이므로 의미가 없지만, 문턱전압이 0.5 mV 이상인 영역에서는 잡음에 의한 펄스와 신호에 의한 펄스가 다르게 나타난 것을 볼 수 있다. 즉, 신호가 발견될 확률은 빛의 세기에 비례하여 조금씩 줄어들었지만 잡음에 의하여 펄스가 발견될 확률은 문턱전압이 0.5 mV 이상에서는 거의 나타나지 않

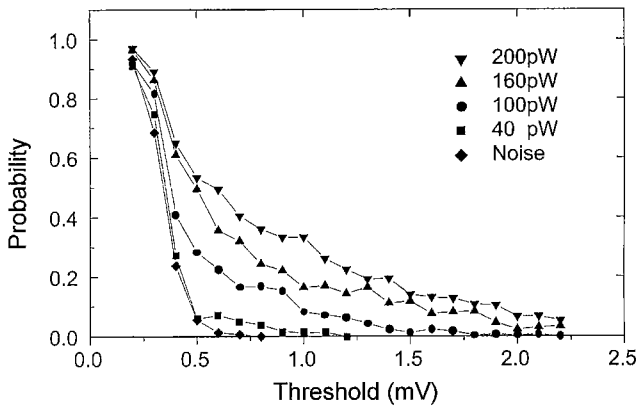

그림 4. 검출기에 91.4 V의 전압을 걸어주고 빛의 세기에 따른 검출기의 반응성능을 측정한 값이다. 여기에서 측정된 빛의 세기는 필터를 포함 시킨 실험장치 전반부에서 측정 한 값이다.

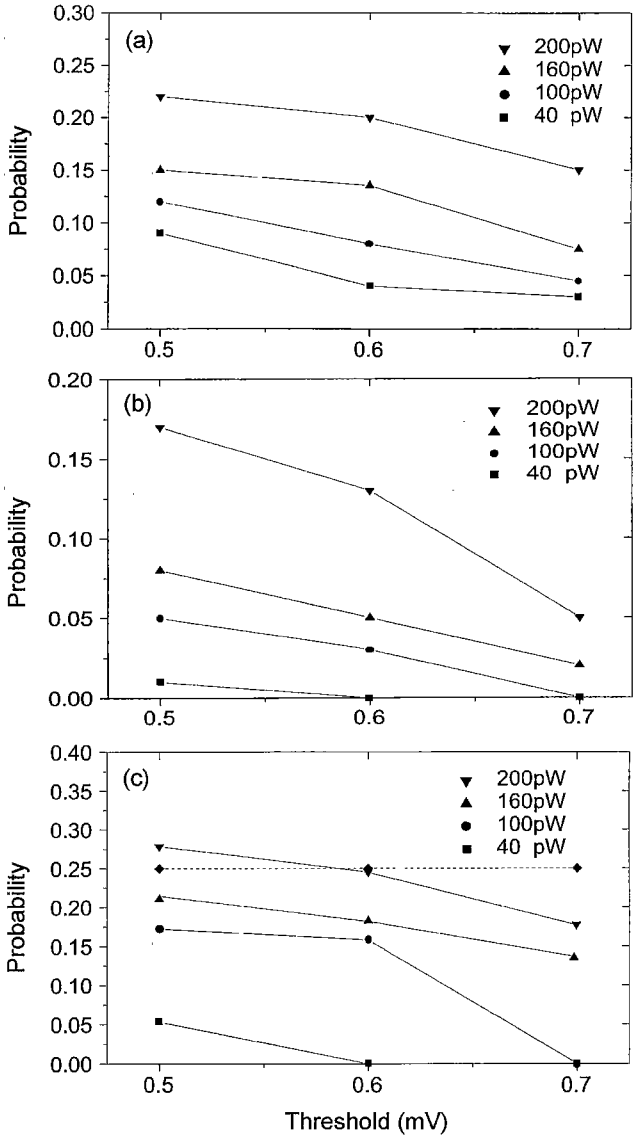

그림 5. (a) 검출기 A에서만 펄스가 발견될 확률, (b) 검출기 A와 B에서 동시에 발견될 확률, (c) 양자 암호화 가능영역.

았다. 그러나 문턱전압이 1.0 mV 이상인 경우 역시 잡음과 신호를 구별 할 수 있는 영역이었지만, 다른 영역에 비교하면 상대적으로 신호가 발견될 확률이 낮은 영역이다. 그림4에서 알 수 있듯이 검출기의 최대 SNR을 갖는 인가전압은 91.4 V 이며 이때 문턱전압의 영역은 0.5 mV에서 1 mV 사이이다.

다음은 위의 문턱전압 영역에 편광된 빛을 보내어 두 검출기 중 하나의 검출기에서만 신호가 발견될 수 있는 빛의 세기를 찾아 각각의 세기에 따른 검출된 확률을 알아보았다. 그림 5(a)는 특정 인가전압 91.4 V에 대하여 문턱전압과 빛의 세기를 조절하여 한쪽 검출기에서 신호가 발견될 확률을 나타낸 것이며 그림 5(b)는 검출기 A와 B에서 동시에 발견될 확률을 나타낸 것이다. 빛의 세기가 센 경우에는 검출기 A와 B로 반반씩 나뉘어져 두 곳 모두에서 신호 측정가능성이 있고 더욱이 문턱전압이 낮을 경우 잡음까지 신호 처리하므로 확률이 높아짐을 알 수 있다. 약한 빛을 하나의 광자처럼 생각했을 때 두 검출기 A, B동시에 측정되어진다는 것은 도청이 가능한 영역이라고 말할 수 있다. 그래서 두 검출기 중 어느 한쪽만 발견될 확률이 높은 영역에서 양자 암호화 키가 사용되어야한다. 만약 이런 조건하에서 송수신자가 정보를 교환할 때 도청자가 있다면 도청에 의한 신호왜곡이 잡음에 의한 신호왜곡보다 더 높게 나타나기 때문에 송수신자는 도청된 사실을 알 수가 있다. 이러한 모든 것을 고려해 보면 잡음에 의한 신호 왜곡률이 25%이하에서 완전한 양자암호화 키를 보낼 수 있다. 그림 5(c)는 잡음에 의한 신호왜곡률을 나타낸 것이며 점선은 도청자가 존재했을 때 도청에 의한 신호왜곡률을 나타낸 것이다. 문턱전압과 빛의 세기를 조절하여 양자효율이 1이 아닌 검출기 한계와 잡음이 존재하는 현실적 문제에서도 양자 암호화가 사용 가능한 영역을 실험적으로 찾아보았고, 이런 범위 안에서 은밀한 정보를 안전하게 보낼 수 있음을 알 수 있다.

여기에서 측정된 빛의 세기는 필터를 포함시킨 실험장치 전반부에서 측정한 값이다. 이 빛이 여러 광학계를 통과하여 아주 약한 세기의 빛이 되어지기 때문에 검출기에 입사된 빛의 세기는 측정이 불가능하였다.

IV. 결 론

고전적인 암호화는 현재까지는 완전한 것처럼 보인다. 그 이유는 도청자가 도청하기 위해서는 현재의 암호화로 되어진 수학적 알고리즘을 해독하는 빠른 컴퓨터와 많은 시간이 필요하기 때문이다. 그러나 수학적 알고리즘을 수 초 이내에 해독할 수 있는 양자 컴퓨터가 등장한다면 고전적 암호화에 의해 송신자가 수신자에게 보내진 정보는 쉽게 도청될 뿐만 아니라 송신자와 수신자는 도청된 사실조차도 알 수 없는 것이 현재의 고전적 암호화이다. 그러나 양자암호화 통신은 고전적 암호화와 달리 자연의 기본적 법칙인 불확정성 원리 등이 그 안전성을 보장한다. 양자 암호화 통신에서 도청자가 정보를 복제하기 위해 신호를 측정한 다면 결국은 신호를 왜곡시키게 된다. 따라서 송수신자는 도청 사실을 감지할 수 있게 된다.

우리는 양자 암호화에 대한 실험 방법 중에서 4가지 편광상태를 이용한 실험을 수행하였다. 광원으로 Nd:YAG 레이저를 이용하였고 송신자의 전기광학변조기와 수신자의 위상지연판을 조절하여 양자 암호화 전송을 수행하였다. 검출기는 Newport사 877 Silicon Avalanche Photodiode를 사용하였다. 실험에서 사용된 빛은 하나의 광자 펄스가 아니지만 하나의 광자 펄스처럼 약한 빛의 세기로 만들었다. 이런 약한 빛에 반응성능을 높이기 위하여 검출기에 인가전압을 주고 추가적으로 신호에 의한 펄스와 잡음에 의한 펄스를 구별할 수 있도록 문턱전압을 조절하여 검출기의 반응성능이 가장 좋은 영역을 찾았다. 양자효율이 1이고 잡음이 없는 경우 이론적으로 완벽하게 암호화 통신이 가능하나 그렇지 않은 경우 즉 양자효율이 1이 아니고 잡음이 섞이게 되는 경우에서 신호와 잡음을 구별할 수 있는 문턱전압과 빛의 세기를 조절하여 양자암호화가 가능한 영역을 찾았다.

양자 암호화에서는 도청자에 의한 신호왜곡과 잡음에 의한 신호왜곡이 존재하게된다. 정보가 도청되어지고 있다면 25%

의 신호왜곡률이 존재하므로 잡음에 의한 신호왜곡은 이것보다 적어야 한다. 만약 잡음에 의한 신호왜곡이 도청의 의한 신호왜곡보다 크면 도청에 의한 신호 왜곡인지 잡음에 의한 신호왜곡인지 알 수가 없게 된다. 본 실험에서 찾아냈던 결과는 25%보다 낮은 신호왜곡 확률이 존재하고 있다는 것을 실험적으로 찾아냈고, 이런 영역 내에서 양자암호화 통신이 가능하다는 것을 알 수 있었다. 여기서 주어진 조건은 수신자와 도청자 모두에게 동일한 실험 장치를 적용한다고 가정하였다

참고문헌

[1] D. E. Denning *Cryptography and Data Security* (Addison-Wesley Publishing company, London, 1982).

[2] C. Ponerance, "A table of two sieves," *Not. Amer. Math. Soc.*, vol. 43, p. 1473, 1996.

[3] P. W. Shor, in *Proceedings of the 35th Annual Symposium on the Foundation of Computer Science* (IEEE Computer Society, Los Alamos , CA, 1994), p. 124.

[4] Y. Nakamura, Yu. A. Pashkin, and J. S. Tsai, *Nature*, vol. 398, p. 768, 1999.

[5] J. I. Cirac and P. Zoller, *Phys. Rev. Lett.*, vol. 74, p. 4091, 1995.

[6] J. Jones and M. Mosca, *J. Chem. Phys.*, vol. 109, p. 1648, 1998.

[7] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, *Journal of Cryptology*, vol. 5, p. 3, 1992.

[8] A. K. Ekert, *Phys. Rev. Lett.*, vol. 67, p. 661, 1991.

[9] C. H. Bennett, *Phys. Rev. Lett.*, vol. 68, p. 3121, 1992.

[10] A. K. Ekert, J. G. Rarity, P. R. Tapster, and G. M. Palma, *Phys. Rev. Lett.*, vol. 69, p. 1293, 1992.

[11] C. H. Bennett, G. Brassard, and A. K. Ekert, *Sci. Am.*, p. 50, Oct. 1992.

[12] W. K. Wooters and W. H. Zurek, *Nature*, vol. 299, p. 802, 1982.

[13] D. Dieks, *Phy. Lett.*, vol. A92, p. 271, 1982.

The efficiency of the quantum key distribution depends on the characteristics of the detector system

Kihyun Cho, Jangwon Kang, and Sun-Hyun Youn†

Department of Physics, Chonnam National University, Kwangju 500-757, KOREA

†*E-mail: sunyoun@chonnam.ac.kr*

(Received November 1, 2000; Revised manuscript received March 20, 2001)

We studied quantum cryptography based on the quantum nature of light. We must reduce the intensity of the light pulse to the single photon regime for quantum cryptographic communication. Considering the noise and the quantum efficiency of the detector, however, we have to find a criterion for which we are able to distinguish the error caused by eavesdropping from other system noises. By changing the bias voltage of the detector and the threshold of the signal voltage, we find the safe region for which we can distribute the quantum key with positive proof of no-eavesdropping. The quantum key we used is a four state quantum key (BB84).

Classification codes : QO.010, QS.010.