초고속정보통신망을 위한 양자 통신시스템의 암호화 기법 분석

김정태
목원대학교

Analyses of Encryption Method of Quantum Communication for High-speed communication

Jung-Tae Kim
Mokwon University
E-mail : jtkim3050@mokwon.ac.kr

요 약

본 논문에서는 양자 통신시스템을 위한 양자 암호화 방법 및 이를 기반으로한 암호 통신시스템을 분석하고, 그 응용 분야에 대한 기법을 해석한다. 이러한 양자 암호화 방업은 기존의 전기 통신망에서 주로 사용되고 있는 여러 가지의 암호화 기법이 속도가 증가됨에 따라, 그 암호화 해독 방법이 깨지고 있는 실정이다. 따라서 본 논문에서는 이를 위한 기본적인 개념을 해석하고 추후 개발하고자 하는 양자 암호시스템을 해석한다.

Ⅰ. Introduction

Quantum cryptography exploits the fundamental properties of quantum complementary to allow two remote parties, Alice and Bob, to generate a shared random bit sequence that is probably secret. This addresses one of the central requirements for communications privacy, since Alice and Bob can safely use their shared bit sequence as key for subsequent encrypted communications. In conventional complexity-based approaches to security, privacy depends on the proposed difficulty of solving certain classes of mathematical problem. In contrast, quantum key distribution provides a new paradigm for the protection of sensitive information in which security is based on fundamental physical laws. This talk will review the current status of QKD and give examples of number of fiber-optic systems that have been built and tested recently in several research. Unfortunately many researcher in chaos-based cryptography, while rushing to publish a novel cryptographic algorithm, come up, although without any cryptographic skills, with both weak and slow ciphers. Most of the chaotic communication system proposed so far need to establish reliable chaos synchronization between a transmitter and a receiver. High quality of chaos synchronization is very important in assuring reliable message recovery. Chaos synchronization has been intensively investigated in many coupled semiconductor laser systems for chaotic optical communication. However, most of the investigation have focused on synchronization of chaos without encoded message. In fact, in chaotic communication, the process of message encoding and decoding can change the quality of chaos synchronization by changing the symmetry between the transmitter and the receiver. Therefore, it is very important to investigate the synchronization of chaos in the process when messages are being encoded and decoded in a chaotic communication system.

Ⅱ. Quantum Cryptography

The following material describes the original quantum key distribution protocol developed by Bennett and Brassard. In general, quantum information systems require the use of some suitable two-state quantum objects to provide quantum-level representations of binary information. In the BB84 scheme, Alice and Bob employ the linear and circular polarization states of single photons of light for this purpose. Figure 1 shows schematic representations of these states together with the notation used to represent them and their associated binary values. The linear and circular "bases" are used to provide two different quantum level representations of zero and one. Before describing how the properties of these single photon polarization states are exploited in the key distribution protocol we will consider the outcomes and interpretation of various possible measurements that can be performed on them. In each case the receive has arranged a polarizer and two single photon detectors to perform a linear polarization measurement on the incoming photon. For the two linear states the outcome of the measurement is deterministic. the $|V>_{\text{linear}}$ photon is registered at detector D_v and the $|H>_{\text{linear}}$ photon is registered at detector D_h both with 100% accuracy. Of course similar results would also be obtained for classical input fields in the vertical and horizontal polarization states. In contrast, a classical input state with circular polarization would generate equal-intensity signals at the two detectors. Single photon, however, are elementary excitation of the *electromagnetic field and they cannot split* in two. Instead the $|R>_{\text{circ}}$ and $|L>_{\text{circ}}$ states behave in a random fashion and have a 50% probability of being repolarized in the state $|V>_{\text{circ}}$ and registered at D_v and, similarly, a 50% probability of being repolarized in the state $|H>_{\text{linear}}$ and registered at D_h. In quantum mechanisms terminology the photon is said to be projected into an eigenstate of the measurement operator, namely, either $|V>_{\text{linear}}$ or $|H>_{\text{linear}}$. Taking he example of the $|R>_{\text{circ}}$ state, the probability of each possible outcome is given by the squared modulus of the amplitude coefficients in

$$|R>_{\text{circ}} = 1 / \sqrt{2} \; (|V>_{\text{linear}} + i|H>_{\text{linear}})$$

the expansion of $R>_{\text{circ}}$ in the linear representation.

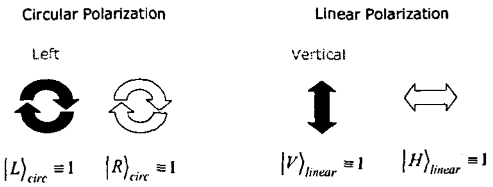

Circular Polarization
Linear Polarization
Left
Vertical
$|L\rangle_{circ} \equiv 1$
$|R\rangle_{circ} \equiv 1$
$|V\rangle_{linear} \equiv 1$
$|H\rangle_{linear} \equiv 1$

Fig 1. Schematic representation and notation of polarization

III. Phase coded quantum cryptography scheme

The quantum channel shown in fig 2 is based on a fiber version of the phase encoded Mach-Zehnder scheme. The laser source is a 1.3um-wavelength distributed feedback laser that is gain switched at 1MHz to produce a train of ~ 100 ps duration pulses. The output of the laser is strongly attenuated so that the intensity at the input to the transmission fiber is in the range 0.1 ~ 0.2 photons per pulse pair, on average. Each attenuated laser pulse enters a 50/50 optical coupler where the pulse splits and some component travels through a lithium niobate modulator and experiences a phase-shift ϕ_A chosen at random from one of the four possibilites, 0^0, 90^0, 270^0, 270^0. The other component travels through a 2ns delay loop and a polarization controller that rotates the polarization into the orthogonal state. The two pulses, now with orthogonal polarization, are fed into the transmission fiber via further 50/50 coupler. Because the 2ns time delay between pulses is small compared to the typical time scales for environmental fluctuations the device can be made interferometically stable even though the transmission fiber is many kilometers in length. At the output of the fiber the two pulses enter Bob's half of the interferometer, where they are spatially separated by a polarization splitter.

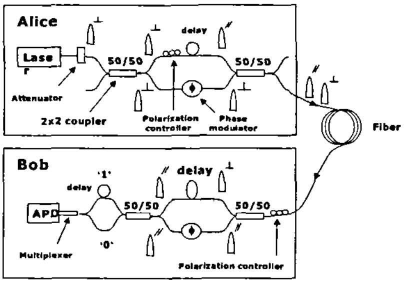


Fig 2. Phase coded quantum cryptography scheme

IV. Simulation Result

The optical injection locking configuration is made up of ML and SL as shown in Fig. 3, where the CW ML light is injected into the SL cavity. Two lasers have a frequency offset of , where is defined as *ML* - *SL*. It is assumed that the injected ML light has the same polarization as SL by the proper control of the polarization controller located between the two lasers. Assuming DFB lasers with negligible sidemodes are used for both ML and SL, the SL under the influence of external light injection can be described by the following single mode rate equations shown below.

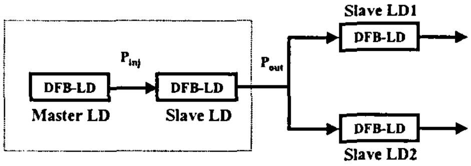


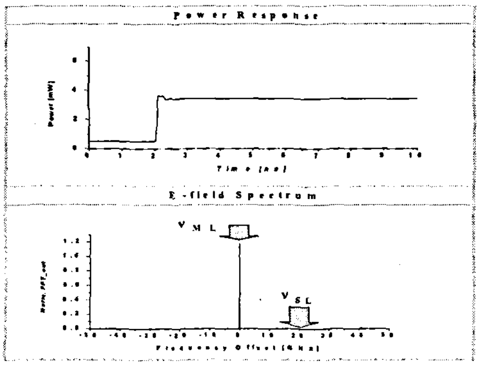
Fig 3. Optical Injection Locking Scheme for Chaos Quantum cryptography

$$\frac{dP}{dt}=\left[\frac{\Gamma g_0}{1+\varepsilon P}(N-n_t)-\frac{1}{\tau_p}\right]P+\frac{\Gamma\beta}{\tau_n}N+2K_C\sqrt{P_{in}P}\cos(\Phi_{ML}-\Phi)$$

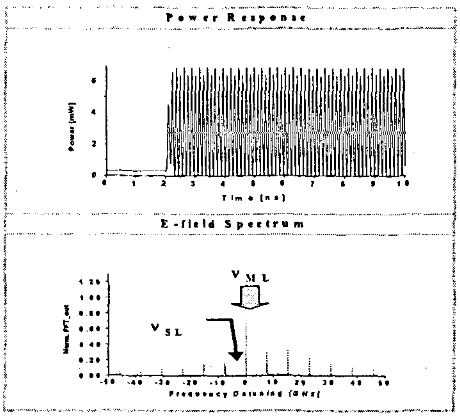
$$\frac{d\Phi}{dt}=-2\pi\Delta f+\frac{1}{2}\alpha\left[\Gamma g_0(N-n_t)-\frac{1}{\tau_p}\right]+K_C\sqrt{\frac{P_{in}}{P}}\sin(\Phi_{ML}-\Phi)$$

$$\frac{dN}{dt}=\frac{I}{qV_a}-\frac{g_0}{1+\varepsilon P}(N-n_t)P-\frac{N}{\tau_n}$$

In the numerical simulation, we have assumed three identical semiconductor lasers for one ML and two SLs in Fig. 3. It is assumed that the ML is modulated at 8 GHz so that the optical spectrum exhibits the 2 sideband power larger than the other sideband power in the optical spectrum, where the average ML power is of 3 mW. We have designated the 2 sidebands as target sidebands of two SLs, whose beat signal frequency is 32 GHz in the RF-spectrum. The ML output power passing through an optical attenuator is injected into two SLs as illustrated in Fig. 4. The adjustment of the ML bias level or the modulation power will change the IM / FM indexes deviating the whole optical spectrum, consequently. By controllingoptical attenuator, the ML injection power can be adjusted with no deviation of the optical spectrum. We have investigated the effect of the unselected sidebands on the spectral characteristics for the different ML powers. In the numerical simulation, we have not considered the path length differences in the path to two SLs from ML and the path to PD from two SLs. The SL transient responses are solved by the fourth order Runge-Kutta integration of the field rate-equations in Eq. Two SLs in Fig. 2 are both assumed biased at 1.96*Ith*, at which they emit the optical power of 5 mW in the free-running state. *Ith*is 33.5 mA, here. Then, one of the two SLs in Fig. 4-12is frequency detuned to become locked to the +2 or, -2 target sideband for the different ML powers. The optical spectra of the locked SL can be obtained from the fast-Fourier transformation (FFT) of the SL output power at the steady-state solution of the transient response. Figure 4 shows the optical and RF-spectra of two SLs, which have the frequency separation of 32 GHz in the free-running state.



(a)



(b)

Fig 4. Optical and RF spectra of two SLs when both are (a) chaos condition and (b) locked condition

V. Conclusion

Chaos condition for quantum cryptography is proposed. The lasers are unidirectionally coupled via their optical fields. Numerical studies demonstrate that the optical injection locking scheme is simulated under chaos and locked conditions.As a result, we numerically demonstrate a novel on/off phase shift keying method opening up new perspectives for applications in communication systems using chaotic carriers.

References

[1] Tilmann H, "On/off phase shoft keying for chaos encrypted communication using external cavity semiconductor lasers". IEEE J. of QE, v.38, n.9, sep. 2002, pp.1162-1170

[2] Shuo T, "Effects of message encoding and decoding on synchronized chaotic optical communication", IEEE J. QE, v.39,n.11, Nov, 1003, pp1468-1474