케이오스 변조기법을 이용한 광학적 암호시스템의 분석

김정태
목원대학교

Analyses of Quantum Cryptography with Chaos Modulation

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

요 약

Quantum cryptography is considered as a promising solution towards absolute security in long term cryptosystems. While the application of quantum cryptography in fiber networks has significant advances, research on the application of quantum cryptography in mobile networks is still prematures. In this paper, we analyses the interests of using quantum technique.

Ⅰ. Introduction

As an application of chaos theory, secure communications have been studied since the early 1990s. Such chaotic properties as ergodicity and sensitive dependence on initial conditions and on system parameters are quite advantageous to construct secure communication schemes including cryptosystems, where irregularity in code sequences, sensitive dependence on plaintexts, and keys are required. The very essence of chaos characterized most commonly as extreme sensitivity to initial conditions makes us believe that chaos synchronization is nearly impossible once. In order to overcome this drawback, different methods have been proposed. In particular, the scheme suggested by Carroll and Pecora consists in taking a chaotic system, duplicating some subsystem and driving the duplicate and the original subsystem with signals from the unduplicated part. When all the Lyapunov exponents of the driven subsystem (response system) are less than zero, the response system synchronizes with the driving system if both systems start in the same basin of attraction. Secure communication protocols based on chaotic masking, chaotic switching and chaotic modulation are most prevalent among chaotic communication techniques. In all of them, the consistency between the transmitter system and the receiver system is ascribed to chaos synchronization.

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>linear photon is registered at detector Dv and the |H>linear photon is registered at detector Dh 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>circ and |L>circ states behave in a random fashion and have a 50% probability of being repolarized in the state |V>circ and registered at Dv and, similarly, a 50% probability of being repolarized in the state |H>linear and registered at Dh. In quantum mechanisms terminology the photon is said to be projected into an eigenstate of the measurement operator, namely, either |V>linear or |H>linear. Taking he example of the |R>circ state, the probability of each possible outcome is given by the squared modulus of the amplitude coefficients in

|R>circ = 1 / √2 (|V>linear + i|H>linear)

the expansion of R>circ in the linear representation.

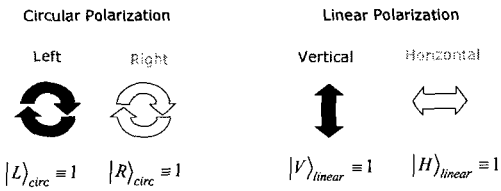

Fig 1. Schematic representation and notation of polarization

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 ϕA chosen at random from one of the four possibilites, 00, 900, 2700, 2700. 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.

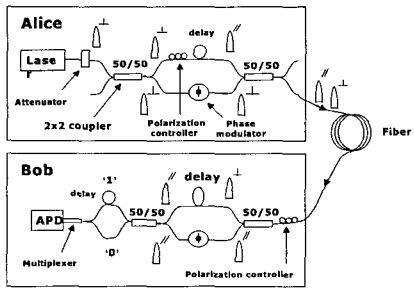

Fig 2. Phase coded quantum cryptography scheme

IV. Quantum Cryptography Technical Issues

Research on QC continues in academia and industry and significant funding has been devoted to prove the viability of quantum cryptography method and particularly the quantum key distribution (QKD). Despite this, currently no off-the-self QC systems exist that are applicable to multi-wavelength (DWDM) fiber communications. As such, the networks that have been established are experimental testbeds consisting of a short single mode fiber less than 2 kilometers to establish a private single-link point-to-point topology [17]. In a general applicability of QC, there will be many issues, which deserve to be identified and examined. These issues are:

1) Single photon generation with the desired polarization state; there are no "off-the-self" sources with controllable single photon rate generation and controllable photon polarization.

2) Polarization does not remain constant but it changes as photons propagate in the fiber medium due to medium non-linearity.

3) Polarizing filters; there are no "off-the-self" fast tunable polarizing filters with zero insertion loss that can control photon polarization reliably; certain clever method based on Faraday mirrors have been developed but they seem complex and impractical in long length fibers.

4) Single photon source that is synchronized with the polarization state of an external filter; this is not known yet.

5) Point-to-point direct fiber link; the link should remain intact without splices, connectors and other optical components that may alter the polarization state of the propagating photon. This imposes a challenge as the fiber over time does not remain intact in its integrity and its

performance.

6) Single wavelength channels; QC and particularly QKD is limited to single wavelength photons and thus to a single optical channel, thus under utilizing the full bandwidth capacity of fiber. To date, only dedicated point-to-point solutions are contemplated and no solutions have been reported in multichannel transmission.

7) Synchronized polarization filters at both ends (both Adam's and Bob's); polarization states of the filters at either end need to be synchronized and also to take into account the propagation speed of photons in the fiber medium. This is a very delicate issue as temperature drifts cause delays thus changing the synchronization between the two filters.

8) Low bit rate transmission results in significant latency in key identification and encrypted message transmission. Because the process of transmitting photons is very slow, few hundred bits per second, and the bit sequence is too long, see issue #10, the process is comparatively slow.

9) Single chance to successfully negotiate the encryption key. If after a QKD process a key is erroneously identified by Alice, or erroneously executed by Bob, neither side will know. This may create an important issue as it defeats the robustness of the encryption purpose.

10) No acknowledgment by Bob that the negotiated encryption key works reliably or correctly. Bob must know if his polarizing filter behaves as prescribed by Alice, and should also know this from the first arriving photon in the encrypted message. Deciding when the first photon arrives is a task with its own.

11) The quantum cryptographic process of key distribution must frequently repeat itself to reinstate possible de-encrypting misalignments.

12) An eavesdropper may easily attack the transmitted polarization states on purpose. The focus in QKD so far to prevent from eavesdropping. However, it is equally important to prevent or countermeasure attacking. An attacker may tap the medium and maliciously destroy the QKD process and thus hamper transmission of the encrypted message. In such case, an eavesdropper is not only a person that needs to "listen" but also one that hinders and deters successful communication between point A and point B; jamming is a well known form of communication deterrence.

V. Conclusions

We presented a critical view of the working of quantum cryptography and quantum key distribution. This technology is based on the polarization of photons, which is not a well controlled quantity over long distances and in multi-channel networks.

References

[1] Tilmann H, "On/off phase shift 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