Annals of the Academy of Romanian Scientists
Series on Science and Technology of Information
ISSN 2066 - 8562 Volume **5**, Number **2**/**2012**

QUANTUM CRYPTOGRAPHY IN CHAOTIC SYNCHRONIZED SYSTEMS

Bogdan-Adrian STEFANESCU[1], Paul STERIAN[2]

Abstract. *In this paper we propose a simulated combination between the advantages of two security systems, a chaotic signal system and a quantum cryptography protocol. We propose a theoretical scheme for implementing the quantum algorithm to send the chaotic key information from the transceiver to the receiver. To create and simulate the chaotic circuits we simulate several components such as an electro-optic modulator (EOM) is driven by a voltage V, larger than its half-wave voltage V_n, so it will operate in a highly nonlinear regime. When the device is powered optically by a monochromatic source S, its response in intensity is well known to yield a nonlinear function* $F(V) = \cos^2(\pi V_B / (2V_\pi) + \phi)$ *which features a number N of extrema given by* $N \approx V_{pp} / V_\pi$, *where V_{pp}, is peak-to-peak driving voltage and* ϕ *is related to the bias voltage V_B by* $\phi \approx \pi V_{pp} / (2V_\pi)$. *The simulation is based on a theoretical experimental setup. The scheme is designed as follows: the chaotic transmitter is formed by an impedance-matched laser diode (LD) - wavelength* λ_0, *with a time-delayed feedback loop containing an electro-optic modulator EOM, powered by a source S, operating nonlinearly. The LD operates above its threshold, in the linear part of its power-current curve. The optical intensity i(t) of LD is modulated around a mean intensity I_0 by the modulation voltage* $s(t) : I(t) = I_0 + i(t)$, *where* $i(t) = \alpha s(t)$ *is the slope of the power-voltage curve of the LD at its operating point. The feedback loop is formed by a detector D_1 and an amplifier (voltage gain g_1), an EOM (half wave voltage V_π, optical transmission γ) powered by an auxiliary optical continuous-wave (CW) source S (power P), a delay line (an optical fiber with a group propagation time T), and a photo detector D_2 (voltage gain g_2). We use the BB84 protocol to encrypt the information used to synchronize the chaotic circuits. The BB84 protocol is described using photon polarization states for transmitting the information. The transmitter (Alice) and the receiver (Bob) are connected through a quantum communication channel that allows quantum states to be transmitted. For the photons this channel is represented either by open space (air) or optical fiber. We simulate the open space channel to minimize the loss or possible interruptions. This quantum protocol is designed with the assumption that an eavesdropper (Eve) can interfere in any way with both receiver and transceiver. This protocol offers security from encoding the information in non-orthogonal states. The quantum indeterminacy represents the fact that these states cannot in general be measured without disturbing the original state. In addition the receiver and transceiver must communicate via a public classical channel, such as radio or internet to send the encryption key. The three methods of securing a communication system – chaos, quantum cryptography and classical communication channel - all combined creates a new way to protect and transmit important messages or information making the channel almost impossible to be eavesdropped and the information to be stolen.*

Keywords: quantum cryptography, chaotic synchronized systems

[1]Academic Center for Optical Engineering and Photonics, Faculty of Applied Sciences, University "Politehnica" of Bucharest, Romania (bogdanadrians@gmail.com).
[2]Prof. Ph.D. Eng., Physics Chair, University "Politehnica" of Bucharest (paul.sterian@yahoo.com).