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).

1. Introduction

We propose a theoretical scheme for implementing the quantum algorithm to send the chaotic key information from the transceiver to the receiver. We simulate a combination between the advantages of two security systems, a chaotic signal system and a quantum cryptography protocol.

Quantum cryptography solves the key distribution problem by allowing the exchange of a cryptographic key between two remote parties with absolute security, guaranteed by the laws of physics. This key can then be used with conventional cryptographic algorithms [18]. If one encodes the value of a digital bit on a single quantum object, its interception will necessarily translate into a perturbation, because the eavesdropper is forced to observe it. This perturbation causes errors in the sequence of bits exchanged by the sender and recipient. By checking for the presence of such errors, the two parties can verify whether their key was intercepted or not. It is important to stress that since this verification takes place after the exchange of bits, one finds out a posteriori whether the communication was eavesdropped or not. That is why this technology is used to exchange a key and not valuable information. Once the key is validated, it can be used to encrypt data. In telecommunication networks, light is routinely used to exchange information. For each bit of information, a pulse is emitted and sent down an optical fiber to the receiver, where it is registered and transformed back into an electronic signal. These pulses typically contain millions of photons. In quantum cryptography, one can follow the same approach, with the only difference that the pulses contain only a single photon. In particular a photon cannot be split into halves [18], [19].

2. The BB84 protocol

The first protocol for QC has been proposed in 1984 by Charles H. Bennett, from IBM New-York, and Gilles Brassard, from the University of Montreal, hence the name BB84 under which this protocol is recognized nowadays. They published their work in a conference in India, totally unknown to physicists.

We shall explain the BB84 protocol using the language of spin 1/2, any 2 level system being equivalent to it. The protocol uses two interlocutors, Alice, as the transmitter, and Bob, the receiver, as well as an eavesdropper, Eve. The photons of use are divided into 4 quantum states that constitute 2 bases, think of the states up |↑i, down |↓i, left |←i and right |→i. Conventionally, one attributes the binary value 0 to states |↑i and |→i and the value 1 to the other two states, and calls the states qubits (for quantum bits). In the first step, Alice sends individual spins to Bob in states chosen at random among the 4 basic states (the spin states |↑i, |↓i, |→i and |←i are identified with the polarization states ”horizontal”, ”vertical”, ”+45 degrees” and ”-45 degrees”, respectively). How she “chooses at random” is a delicate problem in practice, but in principle she could use her free will. The individual spins could be sent all at once, or one after the other (much more practical); the only restriction being that Alice and Bob can establish a one-to-one correspondence between the transmitted and the received spins [1].

Next, Bob measures the incoming spins in one of the two bases, chosen at random (using a random number generator independent from that of Alice). At this point, whenever they used the same basis, they get perfectly correlated results. However, whenever they used different basis, they get uncorrelated results. Hence, on average, Bob obtains a string of bits with 25% errors, called the raw key. This error rate is so large that standard error correction schemes would fail.

But in this protocol Alice and Bob know which bits are perfectly correlated (the ones for which Alice and Bob used the same basis) and which ones are completely uncorrelated (all the other ones). Hence, a straightforward error correction scheme is possible: For each bit Bob announces publicly in which basis he measured the corresponding qubit (but he does not tell the result he obtained). Alice then only tells whether or not the state in which she encoded that qubit is compatible with the basis announced by Bob. If the state is compatible, they keep the bit, if not they disregard it. In this way about 50% of the bit string is discarded. This shorter key obtained after bases reconciliation is called the sifted key. The fact that Alice and Bob use a public channel at some stage of their protocol is very common in crypto-protocols. This channel does not have to be confidential, but has to be authentic. Hence, any adversary Eve can listen to it all the communication on the public channel, but she can’t modify it. In practice Alice and Bob may use the same optical fiber to implement both the quantum and the classical channels. Note that neither Alice nor Bob can decide which key results from the protocol. Indeed, it is the conjunction of both of their random choices which produces the key. [17], [18].

The quantum channel consists of two main modules: Alice and Bob, that communicate either over open air or optical fiber channel, in this case we consider a perfect noiseless channel.

The classical channel is a basic TCP/IP connection (coaxial or UTP cable). The experiments for optical fibers transmissions are also considered.

Let us now consider the security of the above ideal protocol (ideal because so far we did not take into account unavoidable noise due to technical imperfections). Assume that some adversary Eve intercepts a qubit propagating from Alice to Bob. This is very easy, but if Bob does not receive an expected qubit, he will simply inform Alice to disregard it. Hence, in this way Eve only lowers the bit rate (possibly down to zero), but she does not gain any useful information. For real eavesdropping Eve must send a qubit to Bob. Ideally she would like to send this qubit in its original state, keeping a copy for herself.

3. Theoretical simulation setup

We use a chaos generator in the transmitter and in the receiver which is an electro optic modulator (EOM) driven by a voltage V larger than its half-wave voltage, such that it operates in a highly nonlinear regime, i.e., with a transmission curve F(V) with multiple extrema [3][16].

The idea of using EOMs to generate nonlinear dynamics is not new. The first demonstrations were reported in the '80^{s} with optical bistability from a ring configuration consisting of an EOM that is fed back with the signal from the detected light at its output, such that

$$V = F(V) \tag{1}$$

yielding two steady states as F exhibits two extrema [16]. Low-voltage integrated EOMs were then used to obtain F-functions with a higher number of extrema and to demonstrate optical multi stability.

Following these earlier works, Hopf et al. investigated routes to chaos and bifurcation cascades from EOMs operating as chaos generators by introducing a time retardation T in the feedback signal, such that

$$V(t) = F[V(t-T)] \tag{2}$$

The interest of their investigations was primarily focused on the nonlinear regime and the chaotic dynamics of the oscillator. Our studies, by contrast, are specifically focused on the synchronization of two oscillators to encrypt a message within a chaotic carrier [14]. Attempts have been made to synchronize such chaotic oscillators using Pecora and Carroll’s method [13, 16], but no demonstrations of signal transmission have ever been reported.

The reason appears to be that, in this case, there are no rigorous mathematical solutions yielding chaos synchronization in that case [7].

Then the scheme for generating chaos and signal encoding must be different from those previous works. In what follows, we report on the demonstration of a new scheme with an EOM to solve the difficulty associated with chaos synchronization. We use an EOM powered by an auxiliary source to produce the nonlinear F-function, and we use the time-delayed signal thus obtained, mixed with the message $m(t)$, to modulate the intensity of a second laser diode (LD), which is the emitting source depicted in Fig. 1.

At the receiver, an open-loop synchronization scheme derived from a method that we demonstrated earlier is used to recover the original message $m(t)$. As a bonus, the electrooptically induced nonlinearity features multiple extrema that may make attacks difficult with the breaking methods reported so far.

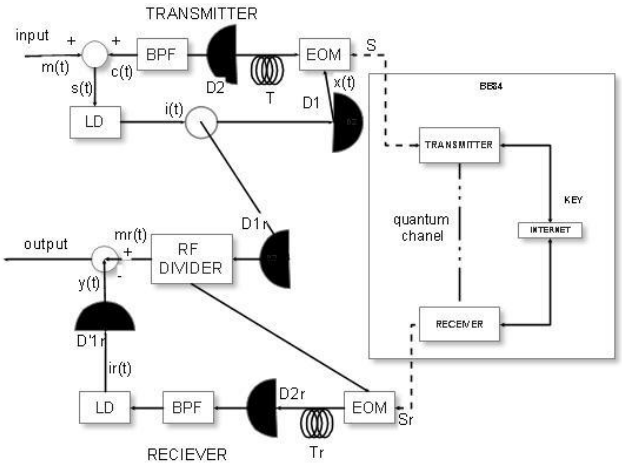

Fig. 1. The simulated system.

The quantum channel consists of two modules, a transmitter and a receiver. The module is designed to produce a stream of single polarized photons according to the choice of basis and bit value. Because no source can produce single photons, we use pulses that have the property of coherency. They are called weak coherent pulses (WCP) of Poisson distribution and mean photon number $\mu = 0.0235$. To produce the pulses, we will use four laser diodes, oriented around a conical mirror at the desired polarization angles. The polarization problem is solved by the laser diodes that have intrinsic polarization. After the beams are reflected by the conical mirror, they pass a spatial filter, which consists of two 100 μm at 0.9 cm apart. It serves a special purpose, that of making the pulse from the four diodes indistinguishable from the others, in spatial terms. This measure has to be taken because without the spatial filtering, the code can be broken quite easily. In order to get as much light as possible through the spatial filter, there is a lens with a focal length $f = 2.75$ mm between the conical mirror and the pinholes of the spatial filter. Because of the very strong spatial filtering, the alignment of the pinholes is crucial, otherwise the desired mean photon count will not be achieved for all polarizations [17].

4. Receiver Module

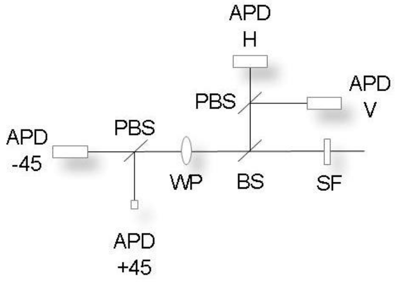

Fig. 1.2. The receiver module.

The module is the heart of the receiver unit is connected directly to a receiver lens and a spatial filter (SF), that are positioned so that the transmitted beam is focused on the primary device of the module. The primary device is an interference filter with a red color glass filter.

This is important to allow for daylight operation, because it rejects stray light, while permitting polarized light to pass. The remaining optical devices divide the photon beams into bases H/V and +/-, the construction being based on the idea by John Rarity and Paul Tapster. An incident photon sees the 50/50 beam splitter (BS). If it is reflected it will see the polarizing beam splitter (PBS) of the photon in the H/V basis, which in combination with the two silicon avalanche photo diodes (APD) H and V. If APD V detects a photon it is supposed to be in the V basis, whereas if APD H detects a photon, it is supposed to be in the H basis. Any photon that is transmitted through the beam splitter passes through a half-wave plate, set at an angle of 22.5, so that it rotates the linear polarization by 45 degrees. Afterwards, a +45 degrees polarized photon is detected by APD 1 and converted into the horizontal basis H, while a -45 degrees polarized photon is detected by APD 3 and converted into the vertical basis V. Whenever a photon is measured in the wrong basis, the measurement outcome is completely random. The APD-s have to be cooled in order to reduce dark counts, at a temperature between -25 and -10 degrees. To reach these temperatures, the photo-diodes are put into an aluminum block which is cooled by a Peltier element glued to it from below. [17]

5. Experimental simulation

In the experiment we consider the message $m(t)$ a signal made of a random sequence of bits. The message signal $m(t)$ is encoded within chaos at the transmitter. The resulting composite signal is sent to a receiver, which performs decoding. The transmitter is formed by an impedance-matched laser diode LD (wavelength λ_0) driven electrically by a feedback loop. 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

$$s(t) : I(t) = I_0 + i(t) \tag{3}$$

where

$$i(t) = \alpha s(t) \tag{4}$$

is the optical intensity fluctuation, and

$$\alpha = dI / ds \tag{5}$$

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 photodetector D_2 (voltage gain g_2).

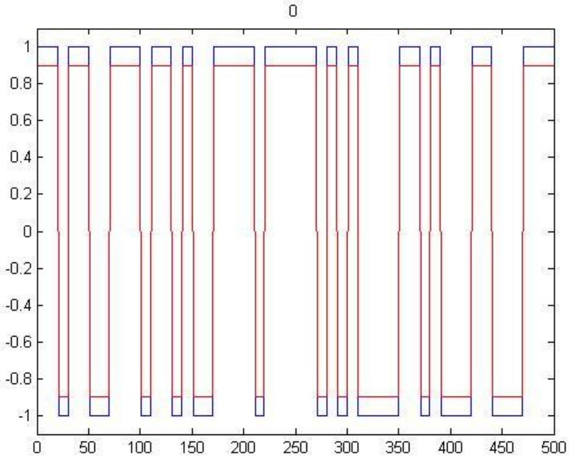

Fig. 2. The input signal – in this case is a random binary sequence, thus to emulate a digital signal.

The transmission curve in intensity of the EOM is the nonlinear F-function

$$F[x(t)] = \frac{P'(x)}{\gamma P} = \cos^2[x(t) + \varphi] \tag{6}$$

where

$$x(t) = \pi V(t)/(2V_\pi) \tag{7}$$

$$\varphi = \pi V_B/(2V_\pi) \tag{8}$$

P'(x) is the optical power at the output of the EOM,

$$V(t) = g_1 i(t) \tag{9}$$

its driving voltage, and V_B is a bias voltage used to adjust its operating point. For generality, we assume that the feedback circuitry features a bandwidth

$$\Delta f = f_1 - f_2 \tag{10}$$

with a high and low cutoff frequency f_1 and f_2, respectively, and behaves as a second-order band pass filter (BPF) (as depicted in Fig. 1) with time constants

$$\tau_1 = 1/2\pi f_1 \tag{11}$$

and

$$\tau_2 = 1/2\pi f_2 \tag{12}$$

The message *m*(*t*) is injected into the feedback loop such that the modulation voltage *s*(*t*) is the addition of *m*(*t*) and the chaotic signal *c*(*t*) at the BPF output [11, 12, 14]:

$$s(t) = c(t) + m(t) \tag{13}$$

with

$$m(t) \ll c(t) \tag{14}$$

This last condition ensures a high masking efficiency as a high degree of security is of concern (this condition comes up at the cost of a reduction of the SNR at the receiver output). The chaotic dynamics of the optical intensity *i*(*t*) emitted by the LD can then be found by considering the different signals in the feedback loop, as we explain below. For simplicity, we consider the second-order BPF as being formed by the combination of a first-order low-pass filter with a 3-dB cutoff at frequency f_1 and a first-order high-pass filter with a 3-dB cutoff at f_2.

Let *v*(*t*) and *c*(*t*) be the input and output voltages of the BPF, respectively. Noting that the output voltage u (t) of the low-pass filter versus its input voltage *v*(*t*) is given by

$$v(t) = \tau_1 \frac{d}{dt} u(t) + u(t) \tag{15}$$

and that the output voltage *c*(*t*) of the high-pass filter versus its input voltage *u*(*t*) is given by

$$u(t) = \frac{1}{\tau_2} \int c(t) dt + c(t) \tag{16}$$

the relationship between the input voltage v(t) and the output voltage c(t) of the BPF is

$$v(t) = \left(1 + \frac{\tau_1}{\tau_2}\right) c(t) + \tau_1 \frac{d}{dt} c(t) + \frac{1}{\tau_2} \int c(t) dt \tag{17}$$

The chaotic dynamics of the transmitter can then be found by noting that c(t) is also the voltage that outputs photo detector D_2 and is therefore related to the optical intensity incident on D_2 by

$$c(t) = \gamma g_2 PF[x(t-T)] \tag{18}$$

with

$$x(t-T) = \pi g_1 i(t-T) / (2V_\pi)\,. \tag{19}$$

It can then be shown from the previous expressions that chaotic fluctuations i(t) occur in the optical intensity of the LD [13], which obeys a second-order DDE (differential delay equations) that can be expressed in the normalized form

$$x(t)+\tau\frac{d}{dt}x(t)+\frac{1}{\theta}\int x(t)dt=\beta F[x(t-T)]+h(t) \tag{20}$$

where $x(t)$ is a dimensionless variable related to $i(t)$, and where the message $m(t)$ is embedded in the trajectories of x(t) via the function

$$h(t)=\frac{\pi}{2V_\pi}\alpha g_1\left[m(t)+\tau\frac{d}{dt}m(t)+\frac{1}{\theta}\int m(t)dt\right] \tag{21}$$

where

$$\tau=\tau_1\tau_2/(\tau_1+\tau_2) \tag{22}$$

and

$$\theta=\tau_1+\tau_2 \tag{23}$$

We observe that a high value of the gains g_1 and g_2 ensures a large bifurcation parameter β, yielding a chaotic solution $x(t)$. (The integral and derivative terms in (25) are physically due to the raising and falling edges of the BPF, respectively). The receiver is formed by the same elements as those in the transmitter, except that the feedback loop is open. In the following, the subscript r refers to the receiver.

The photo detector D_{1r} is illuminated by the intensity fluctuations $Ai(t)$ emitted by the transmitter (A is an attenuation factor related to the optical losses in the transmission fiber) and operates with a gain g_{1r} such that $Ag_{1r} = g_1$, yielding a signal

$$V_r(t)=g_1 i(t) \tag{24}$$

which inputs the modulator EOM. The light beam at the output of EOM, which features the same nonlinear modulation curve F_τ as in (1), is time-delayed by $T_r + T$ and detected by photodiode D_{2r} (gain $g_{2r} = g_2$), yielding a voltage $g_{2r}\gamma_r P'_r F_r[x(t-T_r)]$ at the input of BPF, with $\gamma_r=\gamma$ and $P'_r=P'$ [5].

Following the same procedure as that explained for the transmitter, it can then be shown that the laser diode LD at the receiver features chaotic intensity fluctuations $i_r(t)$, which obey the following normalized second-order DDE:

$$y(t)+\tau_r\frac{d}{dt}y(t)+\frac{1}{\theta_r}\int y(t)dt=\beta_r\cdot F_r[x(t-T)] \tag{25}$$

where

$$y(t) = \pi A g_{1r} i_r(t) / (2V_\pi) \tag{26}$$

$$\tau_r = \tau_{1r}\tau_{2r} / (\tau_{1r} + \tau_{2r}) = \tau \tag{27}$$

$$\theta_r = \tau_{1r} + \tau_{2r} = \theta \tag{28}$$

and [9]

$$\beta_r = \pi A \gamma_r P'_r \alpha_r g_{1r} g_{2r} / (2V_\pi) \tag{29}$$

Noting that $\beta_r = \beta$, one observes that the receiver equation (5) is expressed in the form of (2) when there is no message (*m* = 0) [8].

The receiver behaves, in this case, as a slave generator that replicates the chaos of the transmitter, yielding chaos synchronization i.e. *x*(*t*) = *y*(*t*).

In contrast, when applying the message $(m \neq 0)$, chaos synchronization is lost since we have, from (2) and (5), *x*(*t*) – *y*(*t*) = *m*(*t*) [1].

Therefore, the message *m*(*t*) can be recovered by subtraction of the light intensity $i_r(t)$ of the receiver from the transmitted $i(t)$.

This subtraction is performed electrically at the receiver output [8, 15].

Note that, when *m* = 0, the time to obtain chaos synchronization can be evaluated by considering small deviations δy of *y*(*t*) from *x*(*t*) i.e.,

$$y(t) = x(t) + \delta y(t) \tag{30}$$

yielding

$$\delta y(t) + \tau \frac{d}{dt}\delta y(t) + \frac{1}{\theta}\int \delta y(t) dt = 0 \tag{31}$$

Thus giving

$$\lim_{t\to\infty}[y(t) - x(t)] = \lim_{t\to\infty}[\exp(-\frac{t}{2\tau})] = 0 \tag{32}$$

We observe asymptotically the occurrence of chaos replication [10].

Practically, after a transient time of some 2τ the receiver tracks the chaos produced by the transmitter and the encryption process can begin [6, 7].

Also note that the injection point of *m*(*t*) at the transmitter must be chosen correctly to retrieve the message at the receiver without degradation [14].

The chaotic key is transmitted through a secondary encrypted channel, using the quantum communication BB84 protocol.

6. Simulation conclusions

The idea of this experiment is to understand and to improve the chaos masking of different signals adding a new security module, the quantum channel. The simulated EOMs used were pigtailed Ti:LiNbO integrated Mach–Zehnder modulators with $V_\pi = 3.6\,\text{V}$ at $\lambda = 1540$ nm, an electrical bandwidth of 1 GHz, and with fiber-to-fiber optical losses of – 8 dB (optical transmission $\gamma = 11\%$) [1].

Their electrical bandwidths were not closely matched one with each other. The optical sources were conventional pigtailed laser diodes designed originally for analog CATV fiber transmissions at a 200 MHz frequency. The delay lines were 2 km-long single-mode fibers, yielding a time delay $T = T_r = 0.01\,\text{ms}$. The simulated detectors were InGaAs photo detectors with a sensitivity of 0.9 A/W associated with radiofrequency amplifiers featuring a power gain of 40 dB over a bandwidth of $\Delta f = 142\,\text{MHz}$, ranging from $f_1 = 24.5\,\text{MHz}$ to $f_2 = 166.5\,\text{MHz}$, yielding time constants $\tau_1 = 6.5$, $\tau_2 = 1$, $\tau = 0.9$ and $\theta = 7.4\,\text{ns}$. The gains $g_1, g_2, g_{1\tau}, g_{2\tau}$ were equal to 4 V/mW. The other parameters were the following: $I_0 = 5\,\text{mW}$, $P = 4\,\text{mW}, V_B = 0$ and $\alpha = \alpha_r = 4\,\text{mW/V}$, yielding a bifurcation parameter $\beta = 2.2$. The peak-to-peak driving voltage of the EOMs was $V_{pp} \cong 3V_\pi$, yielding a number of extrema participating to the generation of the chaos equal to $N = 3$ (Fig. 3). The chaotic fluctuations $i(t)$ of the optical power, emitted by the transmitter, are made when the message $m(t)$ is a 100 MHz signal masked within chaos with a message-to-chaos ratio $m(t)/c(t)$ of – 10 dB. The standard deviation of the fluctuations of optical power around I_0 was measured to be 1.3 mW.

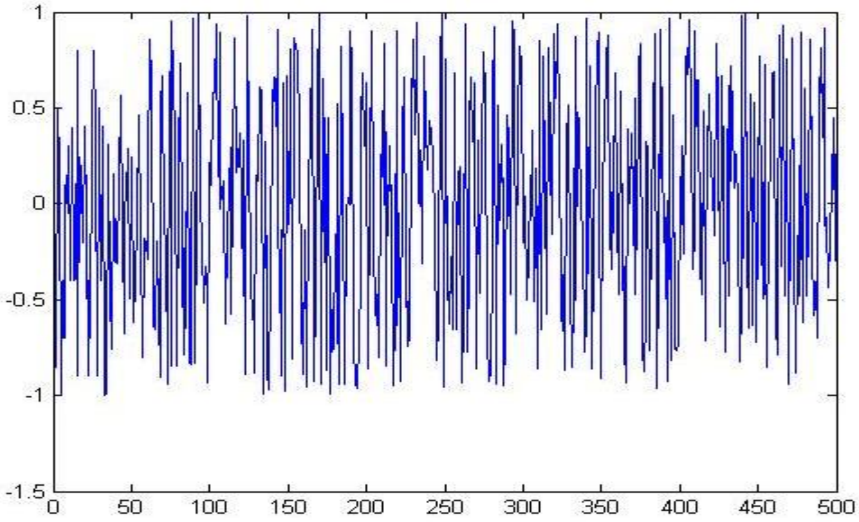

Fig. 3. The transmitted signal over the simulated channel.

The spectrum of $i(t)$ is also the information that an eavesdropper can detect when tapping the transmission fiber. No detectable peak at 100 MHz can be seen in the spectrum.

A proper decoding requires an accurate adjustment of the receiver parameters (bifurcation parameter, filter parameters, time delay, Mach–Zehnder parameters) – the latter form the key parameters – in order to meet the matching conditions required to replicate chaos at the receiver.

Practically, a perfect replication is not possible due to unavoidable mismatches between the components used in the transmitter and receiver.

The message $m_r(t)$ recovered at the receiver is then altered by a chaotic noise.

In the experiments, $m(t)$ was decoded with an SNR of 56 dB as the parameters in the receiver were matched to those in the transmitter with an accuracy better than 1%, except for the gain curves of the RF amplifiers drivers of the EOMs available at the laboratory, which were matched to each other with an accuracy of about 10% only.

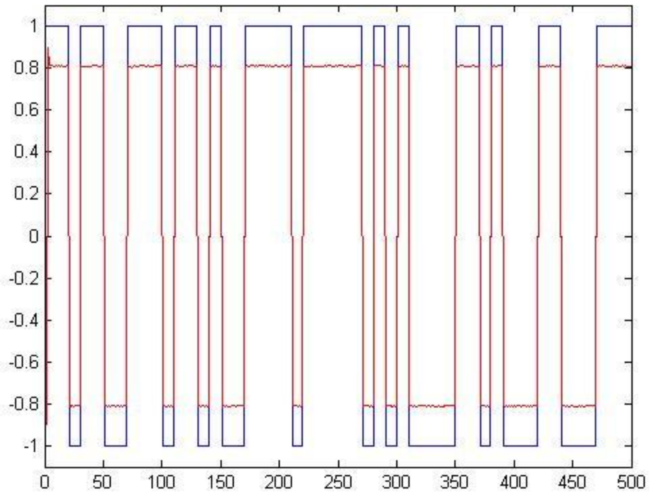

Fig. 4. The received signal – the recovered simulated signal.

In Fig. 5 we may observe the relative low loss of the transmitted signal over the simulated channel.

The simulated transmission channel was a 50 km-long standard single-mode fiber. Fig. 4 gives the recovered signal $m_r(t)$ [1].

The quantum channel is added to the chaotic system to prevent any eavesdroppers to intercept the chaotic key, thus making the system more secure.

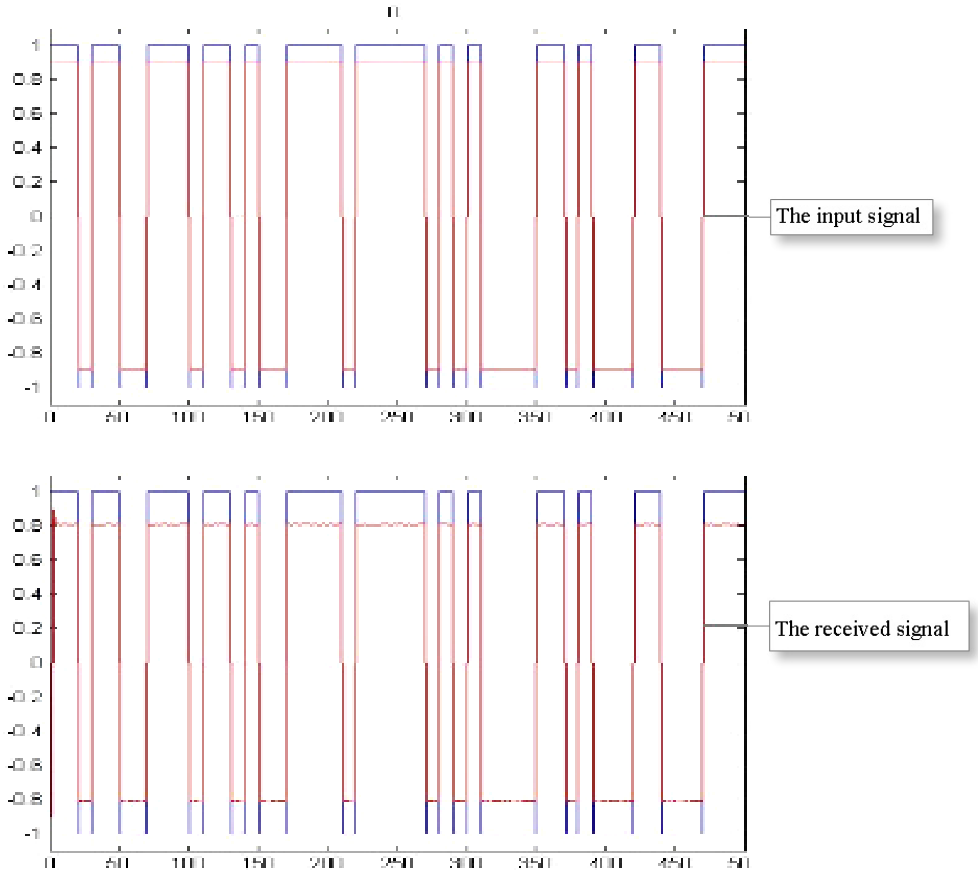

Fig. 5. Transmitted signal vs. received signal.

REFERENCES

[1] Jean-Pierre Goedgebuer, Pascal Levy, Laurent Larger, Chii-Chang Chen, and William T. Rhodes “Optical Communication with Synchronized Hyperchaos Generated Electrooptically”.

[2] S. Hayes, C. Grebogi, E. Ott, and A. Mark, “Experimental control of chaos for communication”, Phys. Rev. Lett., vol. 73, no. 13, pp. 1781–1784, 1994.

[3] L. M. Pecora and T. L. Carroll, “Synchronization in chaotic systems”, Phys. Rev. Lett., vol. 64, no. 8, pp. 821–824, Nov. 1990.

[4] K. M. Cuomo and A. V. Oppenheim, “Circuit implementation of synchronized chaos with applications to communications,” Phys. Rev. Lett., vol. 71, no. 1, pp. 65–68, July 1993.

[5] L. J. Kocarev, K. S. Halle, K. Eckert, L. O. Chua, and U. Parlitz, “Experimental demonstration of secure communications via chaotic synchronization”, Int. J. Bifurc. Chaos, vol. 2, no. 3, pp. 709–713, 1992.

[6] T. Beth, D. E. Lazic, and A. Mathias, “Cryptanalysis of cryptosystems based on remote chaos replication”, in Lecture Notes in Computer Science. Berlin, Germany: Springer-Verlag, 1994, vol. 839, pp. 318–331.

[7] K. M. Short and A. T. Parker, “Unmasking a hyperchaotic communication scheme”, Phys. Rev. E, vol. 58, no. 1, pp. 1159–1162, 1998.

[8] G. Perez and H. Cerdeira, “Extracting messages masked by chaos”, Phys. Rev. Lett., vol. 74, no. 11, pp. 1970–1973, 1995.

[9] L. Kocarev and U. Parlitz, “General approach for chaotic synchronization with applications to communications”, Phys. Rev. Lett., vol. 74, no. 25, pp. 5028–5031, June 1995.

[10] G. Van Wiggeren and R. Roy, “Communicating with chaotic lasers”, Science, vol. 279, no. 3, pp. 1198–1200, Feb. 1998.

[11] J. P. Goedgebuer, L. Larger, and H. Porte, “Optical cryptosystem based on synchronization of hyperchaos generated by a delayed feedback tunable laser diode”, Phys. Rev. Lett., vol. 80, no. 10, June 1998.

[12] J. B. Cuenot, L. Larger, J. P. Goedgebuer, and W. T. Rhodes, “Chaos shift keying with an optoelectronic encryption system using chaos in wavelength”, IEEE J. Quantum Electron., vol. 37, pp. 849–855, July 2001.

[13] L. Larger, J. P. Goedgebuer, V. S. Udaltsov, and W. T. Rhodes, “Radiotransmission system using high dimensional chaotic oscillator”, Electron. Lett., vol. 37, no. 9, pp. 594–595, Apr. 2001.

[14] S. Sivaprakasam and K. A. Shore, “Message encoding and decoding using chaotic external-cavity diode lasers”, Opt. Lett., vol. 24, no. 6, pp. 466–468, 1999.

[15] I. Fischer, Y. Liu, and P. Davis, “Synchronization of chaotic semiconductor laser dynamics on sub-ns time scales and its potential for chaos communication”, Phys. Rev. A, vol. 62, no. 1, pp. 105–110, June 2000.

[16] P. W. Smith and E. H. Turner, “A bistable Fabry-Perot resonator”, Appl. Phys. Lett., vol. 30, no. 6, pp. 280–284, Mar. 1977.

[17] Harald Weinfurter and Alfred Laubereau, “Experimental Quantum Cryptography”, 2003.

[18] Id Quantique, Switzerland, “Securing Networks with the Vectis Link Encryptor”.

[19] Thomas Daniel Jennewein, Anton Zeilinger, “Quantum Communication and Teleportation using Entangled Photon Pairs”, June 2002.

[20] Fernando Lucas Rodriguez, QIT IDE.exe, http://www.fernandolucas.info/QCS, fernandolucas@ieee.org.

[21] Paul Sterian, “Fotonica”, Editura Printech, 2000, ISBN 973-652-161-3

[22] J. L. Duligall, M S Godfrey, K A Harrison, W J Munro and J G Rarity, “Low Cost and Compact Quantum key distribution”, 2006.

[23] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, H. Zbinden, “New Journal of Physics 4”, www.njp.org.

[24] Id 3000 Datasheet v2.1, www.idquantique.com.