13

Chaotic Electronic Circuits in Cryptography

Matej Šalamon
University of Maribor, Faculty of Electrical Engineering and Computer Science
Slovenia

1. Introduction

Chaotic electronic circuits represent deterministic systems which can be used as random number generators in cryptography. Truly chaotic signals can only be generated by analog chaotic circuits. In a cryptosystem a synchronization of the encryption and decryption sides has to be secured, which can be very problematic due to the high sensitivity of the chaotic circuits (Koh & Ushio, 1997; Ogorzalek, 1993). Total inversion of the encryption and decryption sides can only be achieved by using digital chaotic circuits, which act only as pseudo random number generators (Kocarev & Lian, 2011).

In a digital chaotic cryptosystem the chaotic analog circuit is replaced by a suitable mathematic model. The latter is usually represented by equations which are solved with corresponding numerical algorithms, using computers. The digital model of the chaotic circuit therefore represents a mere approximation of its analog variant, and only acts as a pseudo random number generator (PRNG) and not as a truly random number generator (TRNG). Namely, the number of various values is always final in a computer, whereas the values themselves are represented by a limited number of bits.

This article deals with a model of a well-known analog chaotic circuit – the Chua's Circuit, which was used in the cryptosystem as a pseudo random sequence generator. With the mathematical tool Matlab we created a prototype of the cryptosystem and carried out its cryptanalysis. The purpose of the article, however, is not only the presentation of a new chaotic cryptosystem. It tends to point out a few potential problems which can be expected in cryptosystems of this kind.

This article is organised as follows. In the chapter two is presented a phenomenon of chaotic electronic circuits. In the subsequent sub-chapters detailed analysis of chaos in the Chua's circuit is given. The circuit's behaviour is analysed through the three-dimensional state space and the bifurcation diagrams. From the bifurcation diagrams we can read out the parameters at which the circuit's behaviour is chaotic and thus appropriate for random sequences generation. In a cryptographic system, random sequences should be uniformly distributed. Since the basic variant of the Chua's circuit is not able to generate uniformly distributed values, in the continuation the modified Chua's circuit with a more complex chaotic behaviour was introduced. Chaotic state variables in cases of 3-, 4- and 5-scroll chaotic attractors were analysed. All discussed variants of the Chua's circuit were analysed also with the Lyapunov exponents. Based on theirs maximum values, sensitivities to initial conditions were estimated. The most sensitive variant of the Chua's circuit was chosen for the random sequences generator.

The third chapter deals with a usage of chaotic circuits in cryptography. The subsequent sub-chapters describe three basic analog encryption techniques and the structures of a chaos based digital cryptographic system.

The fourth chapter describes the example of digital chaotic cryptosystem with the previously chosen variant of the Chua's circuit. In the sub-chapters are described details of used encryption function and the structure of the entire cryptographic system, adapted for a digital images encryption. In the continuation the cryptanalysis of the described cryptographic system is also presented. Analysis of ciphertexts histograms points out the problem of not uniformly distributed pseudo-chaotic sequences. We have presented also the solution that assures a uniform distribution of pseudo-chaotic sequences. Further we have analysed the statistical and correlation properties of ciphertexts, obtained with different secret keys. Therefore, we performed the auto-covariance and cross-covariance analysis. The problem of a slow initial divergence of pseudo-chaotic sequences is also emphasised. This problem is very evident by an encryption with very similar secret keys.

The last fifth chapter is assigned to the summary of findings and possibilities to solve some problems of the so called chaotic cryptography.

2. Chaotic behaviour of electronic circuits

Electronic circuits can generally be linear or non-linear. As no complete linearity exists in the real world, all circuits are actually non-linear. Their analysis is usually mathematically difficult as it is linked to solving non-linear differential equations.

The multitude of non-linear circuits comprises a huge number of circuits with various behaviour. Concentrating only on autonomous non-linear circuits, we can classify them according to the solutions of equations, describing their behaviour (Ogorzalek, 1997). The solutions can:

- converge to a unique equilibrium point – operating point (RLC-filters, amplifiers etc.);
- converge to one of several possible equilibrium points (bistable circuits, memory cells, sample-and-hold circuits, Schmitt trigger circuits etc.);
- be periodic or quasi-periodic (oscillators, periodic signal generators etc.).

The types of solutions stated above describe the so called »normal« circuit behaviour (Ogorzalek, 1997). However, circuits with a much more exotic – chaotic behaviour have joined the circuits with »normal« behaviour during the last forty years. They are non-linear circuits whose behaviour cannot be determined precisely despite a precise analytic description, as they are high sensitive to initial conditions and some parameters.

Different chaotic circuits have been mentioned in numerous scientific articles like e.g. (Kennedy, 1993a, 1993b, 1994; Sharkovsky & Chua, 1993; Suykens & Vandewalle, 1993; Kolumban & Vizvari, 1994; Šalamon & Dogša, 1995; Hongtao & Zhenya, 1996; Ogorzalek, 1997; Hilborn, 2000). These are simple RLC-circuits, various oscillators, capacitive-trigger circuits, digital filters, flip-flops, adaptive filters, power supplies and converters, power circuits. Figure 1 presents three examples of simple chaotic circuits.

Among the chaotic circuits the most established one – being an object of numerous scientific activities (Chua et al, 1993), is the Chua's oscillator. Kennedy asserts (Kennedy, 1993a,

1993b) that the Chua's oscillator is the only physical system for which the presence of chaos has been established experimentally, confirmed numerically (with computer simulations) and proven mathematically (Chua et al, 1986).

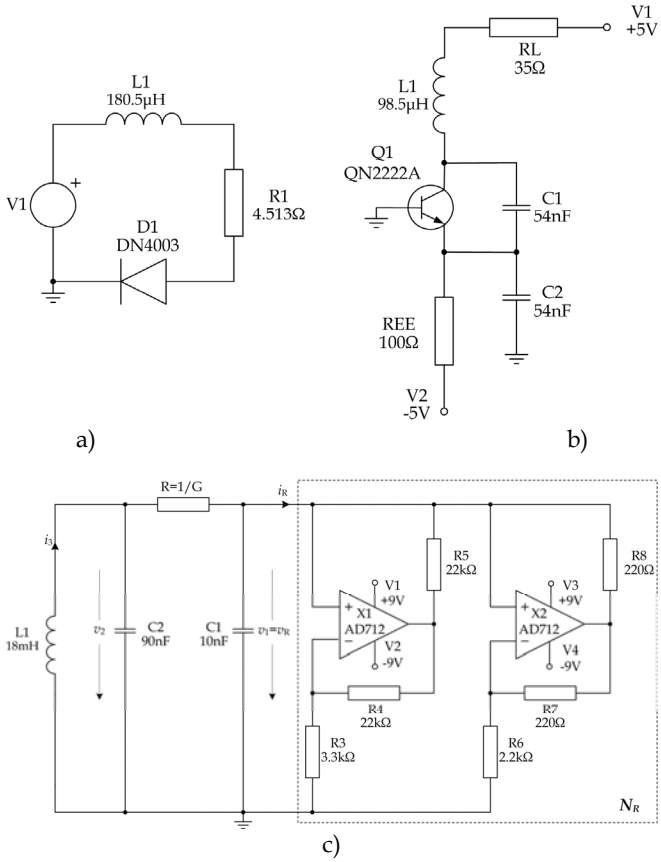


Fig. 1. Examples of simple chaotic circuits: a) diode resonator; b) Colpitts oscillator; c) Chua's oscillator.

Chaotic signals cannot be classified among any of the sorts of solutions of non-linear differential equations stated above. Although their time waveforms are similar to random signals time waveforms, there are substantial differences between them as they are predictable, but only within a short time interval.

The behaviour of chaotic circuits is orderly disordered. Experiments show that in specific conditions (chosen parameters, initial conditions, input signals …) almost all electric and electronic circuits behave chaotically (Ogorzalek, 1997).

Chaotic circuits and other kinds of chaotic systems have certain common characteristics like: high sensitivity to initial conditions, bifurcations, positive Lyapunov exponents, chaotic attractors, fractals etc. (Hilborn, 2000; Sprott, 2009). When using this kind of systems in

cryptography, these characteristics are consequently transferred into cryptosystems. First of all, let us discuss some characteristics of the chaotic Chua's Circuit.

2.1 Chua's circuit

Chua's Circuit, shown in figure 1c, represents an oscillator and a third-order autonomous circuit, respectively (Kennedy, 1993b). It consists of simple electronic components: resistors, inductor, capacitors and operational amplifiers. The *L1* inductor and *C2* capacitor build a resonant circuit, whereas their values determine the basic oscillation frequency. The operational amplifiers *X1* and *X2* as well as the resistors *R3* to *R8* form a voltage-controlled negative resistor (N_R), also called the *Chua's diode* which sustains the oscillation. Basically, the Chua's diode v_R-i_R characteristic has three piecewise-linear segments with two different negative slopes G_a and G_b and two segments with positive slope G_c (figure 2).

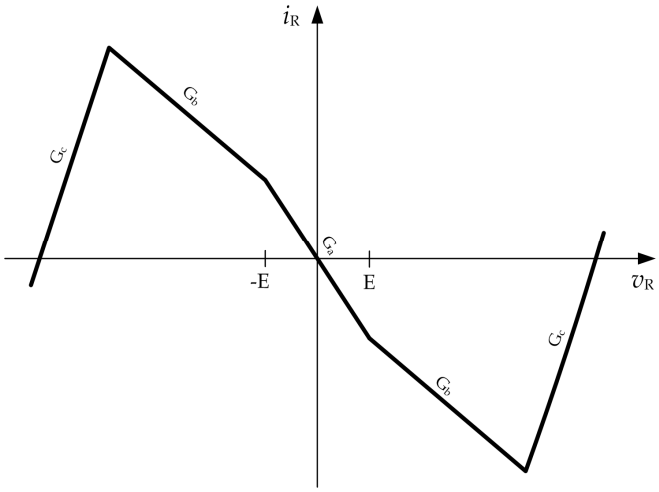


Fig. 2. The Chua's diode v_R-i_R characteristic.

If *R4=R5* and *R7=R8*, the values of the negative slopes of the v_R-i_R characteristic are determined by the equations:

$$G_a = -\frac{1}{R3} - \frac{1}{R6} \tag{1}$$

$$G_b = \frac{1}{R5} - \frac{1}{R6} \tag{2}$$

C1 can be represented as a parasitic capacitor without which the Chua's circuit cannot behave chaotically. Similarly to the resistor $R=1/G$, we can also use the capacitance *C1* as a bifurcation parameter (Kennedy, 1993b). By changing the bifurcation parameter we can influence the behaviour of the Chua's circuit, described by the following differential equations:

$$\frac{dv_1}{dt}=\frac{1}{C1}\left[G\left(v_2-v_1\right)-f\left(v_1\right)\right]=\begin{cases}\dfrac{G}{C1}v_2-\dfrac{G'_b}{C1}v_1-\left(\dfrac{G_b-G_a}{C1}\right)\cdot E & ; \quad v_1<-E\\ \dfrac{G}{C1}v_2-\dfrac{G'_a}{C1}v_1 & ; \quad -E\le v_1\le E\\ \dfrac{G}{C1}v_2-\dfrac{G'_b}{C1}v_1-\left(\dfrac{G_a-G_b}{C1}\right)\cdot E & ; \quad v_1>E\end{cases}$$

$$\begin{aligned}\frac{dv_2}{dt}&=\frac{1}{C2}\left[G\left(v_1-v_2\right)+i_3\right]\\ \frac{di_3}{dt}&=-\frac{1}{L1}v_2\end{aligned} \quad . \tag{3}$$

Here v_1, v_2 and i_3 are state variables. The rest of the parameters are: $G=1/R2$, $G'_a=G+G_a$ and $G'_b=G+G_b$.

A detailed analysis of the Chua's circuit follows, enabling a better understanding of its features and showing possibilities of its use in cryptography.

2.2 The model and the analysis of the Chua's circuit

The analog electronic circuits are usually analysed with analog electronic circuit simulators. SPICE simulators are the best known ones. Up to a certain degree also the chaotic behaviour of circuits can be analysed by them. They can predominantly be used for the time analysis of the voltage and currents in circuits, and also of the so called bifurcation diagrams, given an additional spice macro model (Šalamon & Dogša, 2009).

The use of mathematical tools is necessary for a more detailed analysis of chaotic circuits. The circuit must be described by a suitable mathematical model – by corresponding differential equations. The solution of the equations is carried out by a mathematical tool which – beside the basic time analysis of the state variables – also enables the determination of the bifurcation diagrams, Lyapunov exponents, Poincare's sections of attractors etc.

A more detailed analysis of Chua's Circuit cannot be carried out with an electronic circuit simulator. Therefore we used the mathematical tool Matlab where we initially described the Chua's Circuit by a corresponding model. We used the so called normalized dimensionless form of the Chua's equations (Fortuna et al, 2009). These are acquired by introducing new variables: $x=v_1/E$, $y=v_2/E$, $z=i_3/(E\cdot G)$, $\tau=t\cdot G/C2$, $a=G_a/G$, $b=G_b/G$, $\alpha=C2/C1$, $\beta=C2/(L1\cdot G^2)$ into the equations (3):

$$\begin{aligned}\dot{x}&=\alpha\left[y-x-g\left(x\right)\right]\\ \dot{y}&=x-y+z\\ \dot{z}&=-\beta y\end{aligned} \quad . \tag{4}$$

Here the following function is marked as g(x):

$$g\left(x\right)=\begin{cases}bx+b-a, & x\le -1\\ ax, & \left|x\right|<1\\ bx+a-b, & x\ge 1\end{cases} . \tag{5}$$

Let us also define the following function:

$$h(x) = x + g(x) = m_1 x + \frac{1}{2}(m_0 - m_1)\left(|x+1| - |x-1|\right) \tag{6}$$

which represents the piecewise-linear characteristic (figure 3) with two negative slopes: m_0=a+1 in m_1=b+1.

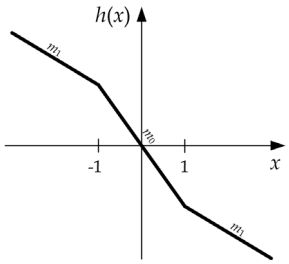


Fig. 3. Piecewise-linear characteristic *h(x)*.

Considering the function *h(x)* in the equations (4) we can describe the Chua's Circuit by an equivalent form of Chua's equations:

$$\begin{aligned} \dot{x} &= \alpha\left[y - h(x)\right] \\ \dot{y} &= x - y + z \\ \dot{z} &= -\beta y \end{aligned} \tag{7}$$

We have analysed the Chua's Circuit behaviour with solutions of the differential equations shown above. The solutions of the equations are represented by the state variables time waveforms: *x(t)*, *y(t)* and *z(t)*. These are equivalent to the voltage time waveforms $v_1(t)$, $v_2(t)$ and the current time waveform $i_3(t)$ in the circuit as shown in figure 1c.

The analysis was carried out at different parameters a and β which in a real circuit depend on the values of the circuit components *R*, *C1*, *C2* and *L1*. We chose the following constant values of the elements: *C1*=10nF, *C2*=90nF, *L1*=18mH and the parameters of the Chua's diode: m_0=-1/7, m_1=2/7. The resistance *R* is variable and represents a bifurcation parameter to which the circuit is very sensitive. By changing it we achieve an alteration of the circuit's global behaviour. According to the selected values of elements parameters: a=9 and β=5·10^{-6}·R^2 can be calculated.

The solutions of Chua's equations can be presented by trajectories in the three-dimensional state space. Some of them are shown in figure 4. The Chua's Circuit at the value of β>15.4 behaves as a common harmonic oscillator. In this case the trajectory represents a limit cycle, shown in figure 4a. At the value of β=16.4 a doubling of the period occurs and the presence of bifurcations, respectively, where the state variables have two different amplitudes. Within the state space, the trajectory only ends after two turns (figure 4b). The reduction of parameter β causes a further orbit splitting, thus causing the formation of period 4, period 8, period 16 etc. Figure 4c presents the period 4, where individual state variables have four different maximum values. By reducing parameter β the orbit splitting becomes more and more frequent, up to the formation of the orbit with an infinite period, which represents the chaotic regime of the circuit operation. This is achieved at the parameter value of β=15.4. In this case an unusual spiral

Chua's attractor appears in the state space, its form being shown in the figure 4d. The trajectory which in such cases never closes, encircles one of the three virtual equilibrium circuit states (Kennedy, 1993b). A further reduction of the parameter β causes the transition of the spiral Chua's attractor into a double-scroll Chua's attractor (figure 4f). Here the trajectory randomly traverses and circles around two different virtual states.

The chaotic regime of the circuit operation is interrupted by several narrow so called »periodic windows« within the Chua's Circuit periodically oscillates again. Figure 4e presents an example of a periodic window, described by a closed trajectory within the state space. Given a small change of the bifurcation parameter, the periodic window disappears and the circuit begins to oscillate chaotically again.

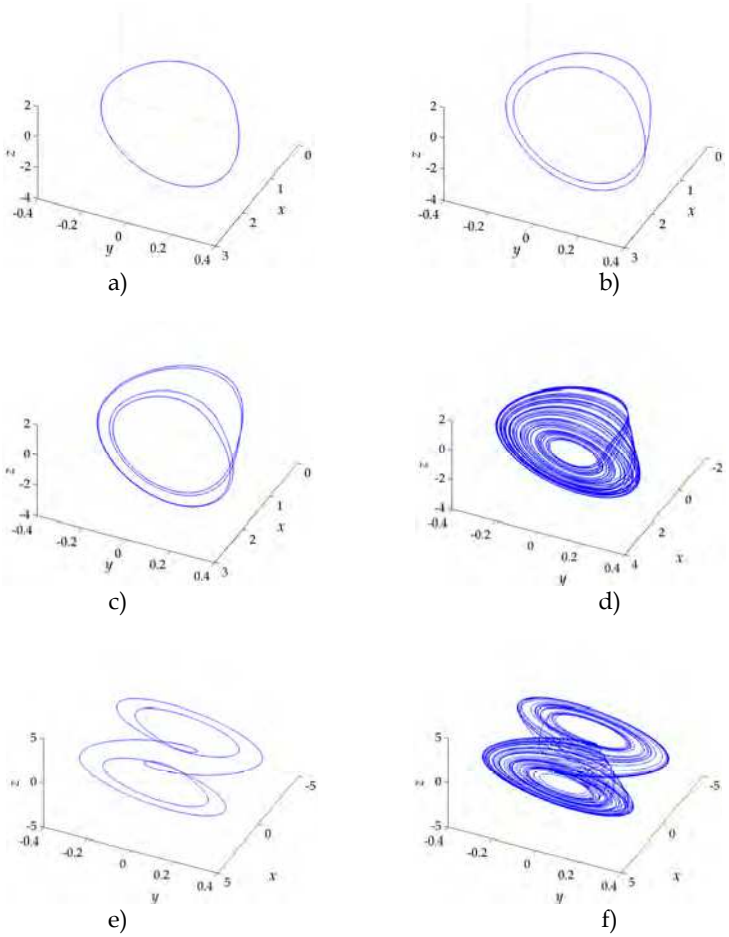


Fig. 4. The behaviour of the Chua's Circuit at different values of the bifurcation parameter β: a) limit cycle (β =17); b) period 2 (β =16.2); c) period 4 (β =15.7); d) spiral Chua's attractor (β =14.9); e) periodic window (β =14.31); f) double-scroll Chua's attractor (β =14.2).

The circuit behaviour described above can be more explicitly presented through the bifurcation diagrams. Bifurcation diagrams of state variables x, y and z are shown in the figure 5. The number of maximum extreme values depends on the bifurcation parameter β. The dark spaces in the bifurcation diagrams represent the chaotic regime of the circuit operation. This regime is interrupted by periodic windows, showing as light spots among dark chaotic areas.

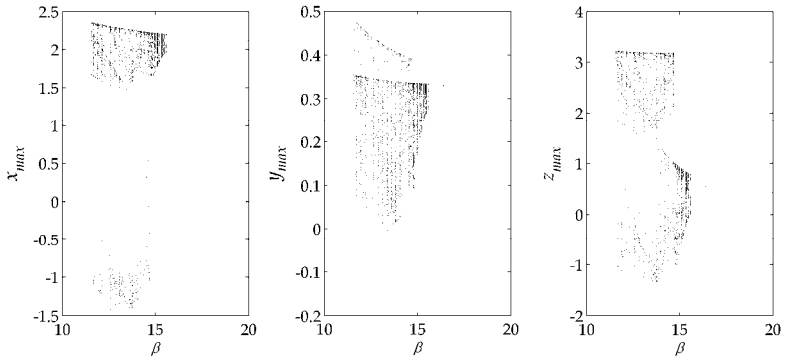
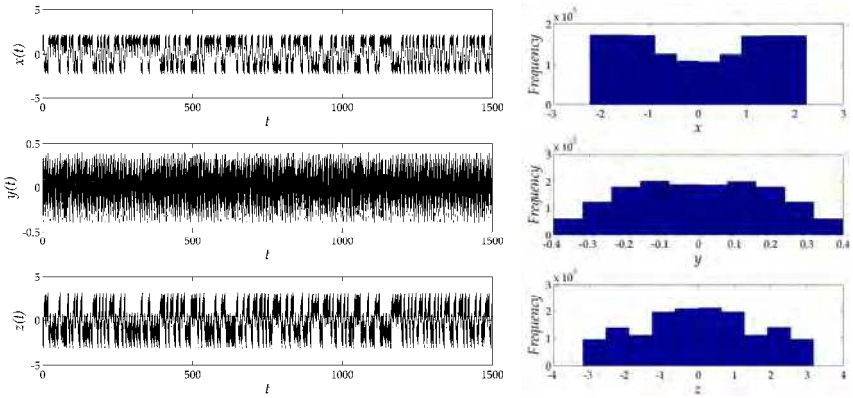


Fig. 5. The Chua's circuit bifurcation diagrams of the state variables x, y and z.

From the cryptographic point of view only the chaotic behaviour of the Chua's Circuit is interesting, being that random signals can only be generated in this mode of operation. It is the characteristics of chaotic signals that although they are non-periodic, certain patterns can be traced in them which do not appear in truly random signals.

Figure 6a shows an example of the state variables time waveforms $x(t)$, $y(t)$ and $z(t)$ in the chaotic regime of the Chua's Circuit operation, described by the double-scroll Chua's attractor; figure 6b shows the corresponding histograms – statistical distribution of the chaotic state variables. We can see that they are not uniformly distributed, showing that some time signal values are more probable than others.



a) b)

Fig. 6. a) The state variables waveforms by the double-scroll Chua's attractor (β=14.2); b) Histograms of the state variables.

On the basis of the analysis results so far obtained we can conclude that it is possible to generate random signals with the Chua's Circuit, but their individual time values will not be uniformly distributed. As this is one of the characteristics required in the random number generators in cryptosystems, which we wanted to come as close to as possible with the Chua's Circuit, we subsequently modified the basic Chua's Circuit (figure 1c). We wanted to achieve more complex circuit dynamics and a uniform distribution of time values.

2.3 The model of the Chua's circuit with a more complex chaotic behaviour

A more complex chaotic behaviour of the Chua's Circuit can be obtained by modifying the Chua's diode characteristic or by a modification of the function $h(x)$, defined by the equation (6). Suykens and Vanewalle ascertained in their article (Suykens & Vandewalle, 1993) that with the Chua's Circuit even more complex signals or more complex attractors can be generated. This can be achieved with several additional segments of the Chua's diode characteristic which is in such cases described by the following function:

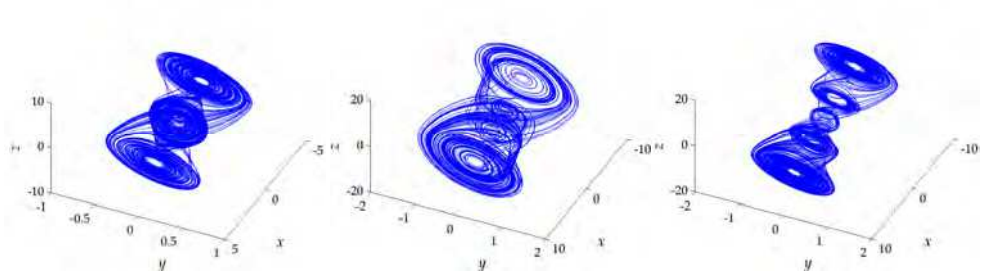
$$h(x) = m_{2q-1}x + \frac{1}{2}\sum_{i=1}^{2q-1}(m_{i-1} - m_i)\left(|x + c_i| - |x - c_i|\right) \tag{8}$$

Here q is a natural number, c_i is the breakpoint of i-th segment and m_i is the slope of i-th segment of the piecewise-linear characteristic $h(x)$. Thus n-scroll or multi-scroll chaotic attractors with n=1, 2, 3… scrolls can be achieved with the Chua's Circuit.

More complex attractors also represent more complex time waveforms of voltages and currents in the Chua's Circuit. Different attractors can be obtained by choosing appropriate breakpoints and slopes of the characteristics $h(x)$ and with suitable parameters α and β. In our case we have limited ourselves to discussing the variants of the circuit with a 3-, 4- and 5-scroll chaotic attractor at the following parameters:

- 3-scroll chaotic attractor: α=9; β=100/7; m_0=0,9/7, m_1=-3/7, m_2=3.5/7, m_3=-2.4/7, c_1=1, c_2=2.15, c_3=4;
- 4-scroll chaotic attractor: α=9; β=100/7; m_0=-1/7, m_1=2/7, m_2=-4/7, m_3=2/7, c_1=1, c_2=2.15, c_3=3.6;
- 5-scroll chaotic attractor: α=9; β=100/7; m_0=0.9/7, m_1=-3/7, m_2 =3.5/7, m_3=-2/7, m_4=4/7, m_5=-2.4/7, c_1=1, c_2=2.15, c_3=3.6, c_4=6.2, c_5=9.

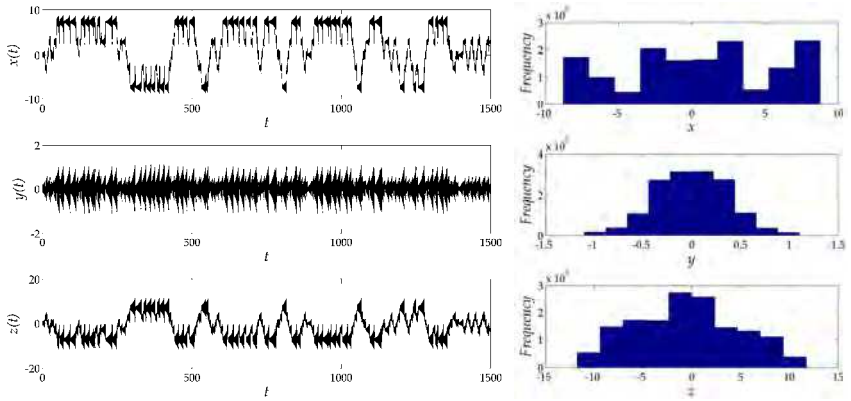
Figures 7a-c show obtained 3-, 4- and 5-scroll chaotic attractors.



a) ` b) c)

Fig. 7. a) 3-scroll chaotic attractor, b) 4-scroll chaotic attractor and c) 5-scroll chaotic attractor.

Figure 8a shows the time waveforms of the state variables $x(t)$, $y(t)$ and $z(t)$ in the case of the 5-scroll chaotic attractor, and figure 8b shows statistical distributions of their time values.



a) b)

Fig. 8. a) Time waveforms of the state variables in the 5-scroll chaotic attractor (β=14.2); b) Histograms of the state variables.

The results show that despite the more complex chaotic behaviour of the Chua's Circuit the time values of the state variables are not more uniformly distributed than in the case of the two-scroll attractor. Despite this fact we used the variant of the Chua's Circuit with a 5-scroll chaotic attractor in planning the encryption system, described later in the article. This circuit variant enabled us the fastest divergence of two trajectories; the evaluation was carried out with the Lyapunov exponent analysis.

2.4 Lyapunov exponents analysis of the Chua's circuit

The basic feature of all chaotic systems is high sensitivity dependence to initial conditions and some system parameters. This feature prevents a long-term prediction of their behaviour. The chaotic trajectories, starting in the state space from close initial conditions, begin to diverge very quickly from each other as time progresses. The speed of their divergence which occurs due to infinitesimal deviation in the initial conditions is evaluated with the Lyapunov exponent (Hilborn, 2000; Sprott, 2009).

The positive Lyapunov exponent is characteristic of all chaotic systems. A higher value of the Lyapunov exponent represents a higher divergence speed of two adjacent trajectories in the state space or more sensitive and faster changing of the chaotic variables. The negative value of the Lyapunov exponent represents a periodic behaviour of the system, whereas the value zero represents the presence of bifurcations which do not represent chaotic behaviour either.

The calculation of the Lyapunov exponent calls for the use of an appropriate mathematical tool and procedure. In our case the Lyapunov exponents were calculated with a procedure suggested by Sprott (Sprott, 2009). Using the Matlab tool, we calculated the average values of the Lyapunov exponents for all four previously discussed variants of the Chua's Circuit at a constant parameter a=9 and at a variable bifurcation parameter β. Figure 9 shows the obtained average values of the Lyapunov exponents λ in the case of the Chua's Circuit with 2-, 3-, 4- and 5-scroll chaotic attractor at various parameter β values.

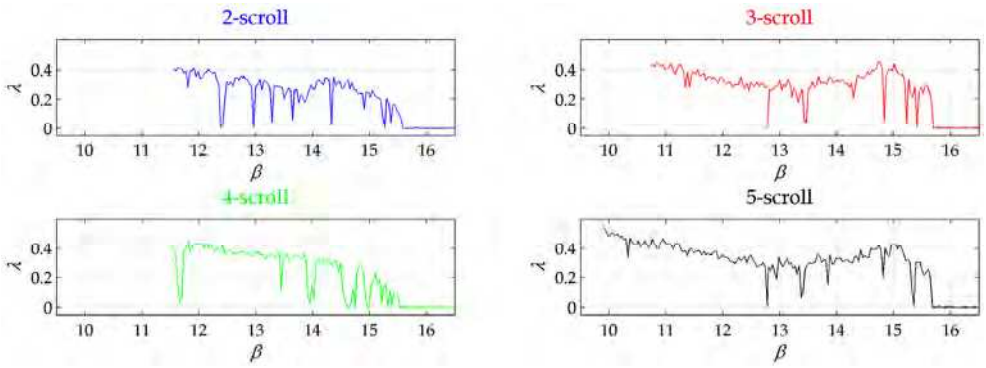


Fig. 9. Average values of the Lyapunov exponent λ vs. β calculated for the Chua's Circuit with 2-, 3-, 4- and 5-scroll chaotic attractor.

The results show that the values of the Lyapunov exponent slightly rise with the complexity of the attractors. Maximum values of the Lyapunov exponents are written in table 1.

	2-sroll	3-scroll	4-scroll	5-scroll
λ_{max}	0.4125	0.4461	0.4467	0.5412
ß	11.6280	14.7620	11.8080	9.9000

Table 1. Maximum values of the Lyapunov exponent, achieved by the 2-, 3-, 4- and 5-scroll chaotic attractor of the Chua's Circuit.

According to the presented dependency of the Lyapunov exponents and their maximum values we can conclude as follows:

- the value of the maximum Lyapunov exponent of the Chua's Circuit with a 5-scroll chaotic attractor is by 31% higher than with a 2-scroll attractor. By a more complex behaviour of the Chua's Circuit faster divergence of the state variables can be achieved;
- individual positive values of the Lyapunov exponent are comparatively small – in the case of a truly random sequence the values of the Lyapunov exponents would be infinitely large;
- Lyapunov exponent values depend largely on the parameter β. In an encryption system it can be a part of the secret key, which in our case cannot be an arbitrary value. Namely, there is a large number of very small and even negative values of the Lyapunov exponent where the Chua's Circuit would surely not behave chaotically;
- if the bifurcation parameter represents a part of the secret key, in the case of the Chua's Circuit there is a strong probability of selecting the so called weak keys which prevent safe ciphering. Namely, the chaotic regime of the circuit operation is limited to several relatively narrow areas, interrupted by periodic windows. They can only be avoided by precise knowledge of the Chua's Circuit behaviour.

The presented results of the analysis of Chua's Circuit indicate problems which can be expected when using it in cryptography. The same problems are also to be expected in the case of other chaotic circuits.

3. The principles of chaotic encryption

When the phenomenon of chaos was discovered in the electronic circuits, questions about the possibility of their use in practice appeared. The similarity among chaotic signals, generated by deterministic systems and random signals which cannot be generated by deterministic systems, led many researchers to the idea of the applicability of chaotic circuits in cryptography. In the beginning, mostly analog cryptosystems were used. Three basic encryption techniques appeared where a complete synchronization of chaotic circuits of the encryption and decryption sides is needed. Due to high sensitivity to initial conditions, external impacts (temperature, noise, ageing of components) and the tolerances of the components, analog chaotic circuits cannot be completely synchronized. Despite this fact analog chaotic encryption proved to be useful predominantly in ciphering undemanding audio signals.

Besides the analog chaotic encryption systems there are also the digital ones. Here instead of truly chaotic analog circuits their discrete models are used. In such cases we are dealing with a digital chaos-based cryptosystems (Kocarev & Lian, 2011).

3.1 Analog encryption techniques

Through the years the following techniques of the analog chaotic encryption were predominantly carried into effect (Dedieu et al. 1993; Ogorzalek, 1993; Koh & Ushio, 1997):

- chaotic masking where the continuous chaotic signal is added to the input analog signal,
- chaotic modulation where the input analog signal is modulated by the chaotic carrier,
- chaotic switching – also known as CSK (Chaotic Shift Keying) where the input digital signal is ciphered by switching between two different attractors. Also the chaotic phase-shift keying – CPSK, and the modulation on the basis of M-synchronized chaotic systems – M-CPSK, are based on the principle of chaotic shifting.

Chaotic masking and chaotic modulation are used at ciphering analog signals while the technique of chaotic switching is used in the case of ciphering digital signals.

3.1.1 Chaotic masking

This is the simplest encryption method where the analog input signal *i(t)* is masked with a chaotic signal *k(t)*. The transmitter contains a chaotic circuit – a generator of a chaotic signal which generates the signal *k(t)*. The latter is added to the signal *i(t)* and then sent to the receiver (figure 10).

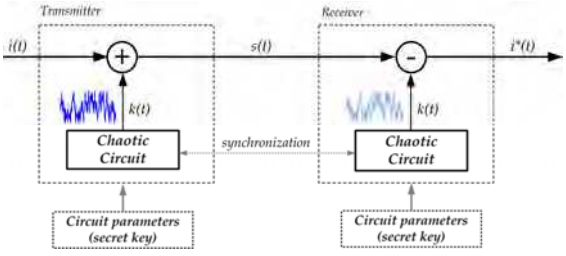


Fig. 10. The principle of chaotic masking.

The masked or ciphered signal *s(t)* is deciphered on the receiver side in the way that the chaotic signal *k(t)*, which has to be the same as the one on the receiver side, is subtracted from it. The signal *i*(t)* shall only be equal to the signal *i(t)* when the transmitter and the receiver have equal and time synchronized chaotic signal generators at their disposal. Further information on the synchronization of chaotic circuits and various methods of synchronization can be found in the literature (Cuomo et al., 1993; Ogorzalek, 1993).

3.1.2 Chaotic modulation

The essence of the chaotic modulation is the modulation of the input signal *i(t)* by a chaotic signal *k(t)* generated by the chaotic signal generator. The signal *i(t)* is modulated by the signal *k(t)* in the chaotic modulator where their multiplication occurs. The modulated signal *s(t)* is transmitted over the communication channel to the receiver where in the chaotic demodulator the demodulation or division of the modulated signal *s(t)* with the chaotic signal *k(t)* is carried out. The equality of the receiver's and the transmitter's parameters and their synchronization is a condition for successful demodulation (Dedieu et al. 1993; Ogorzalek, 1993).

3.1.3 Chaotic switching

The method of chaotic switching represents the simplest form of modulation with chaotic attractors. It is suitable for deciphering digital signals. Let's observe a case of ciphering a binary input signal *i(t)*, shown in the figure 11.

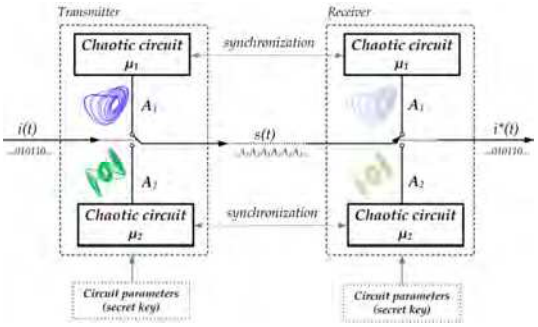


Fig. 11. The principle of the chaotic switching.

The signal *i(t)* controls the switch which toggles between the chaotic systems with different parameters μ_1 and μ_2.

The transmitter consists of two chaotic subsystems:

- the subsystem with the parameters μ_1 – active when *i(t)* = 0,
- the subsystem with the parameters μ_2 – active when *i(t)* = 1.

Transmission of the chaotic attractor A_1, generated by the first chaotic circuit (with the parameters μ_1), corresponds to the logical zero, transmission of the attractor A_2, generated by the second chaotic circuit (with the parameters μ_2), corresponds to the logical one. The entire system acts as a switch which switches between the attractors A_1 and A_2.

The receiver also consists of two chaotic subsystems which have to be identical to and synchronized with the ones on the transmitter side. The first one is designed for demodulating the zeros, the second one for the ones. The demodulation is carried out on the basis of decisions within an individual time interval. A successful demodulation of a logical zero or one is only possible when the chaotic systems on the transmitter and the receiver sides are precisely synchronized (Cuomo et al., 1993; Ogorzalek, 1993; Corron & Hahs, 1997; Yang & Chua, 1996).

3.2 Digital chaotic cryptosystems

Nowadays digital cryptosystems are predominantly used. In general they are divided into symmetric and asymmetric ones (Schneier, 1996; Stallings, 1999). The symmetric ones which only use one secret key, are divided into stream and block systems. The asymmetric ones use two secret keys, the public and the private key.

Chaotic circuits and their digital models, respectively, can be included in any sort of cryptosystems. Here a "naturally" digital chaotic circuit can be used (Šalamon & Dogša, 2000), (e.g. a digital filter), or an analog chaotic circuit can be digitalized.

The digital cryptosystem has several advantages over the analog one:

- it enables complete inversion between the encryption and decryption sides;
- the encryption and decryption algorithms can easily be changed and updated as it is usually implemented with a programme code;
- there is no need for the problematic synchronization of the analog chaotic circuits;
- the digital structure is insensitive to numerous disturbances like the ageing of elements, temperature, noise . . .

The basic structure of the digital chaotic cryptosystem is evident from the figure 12.

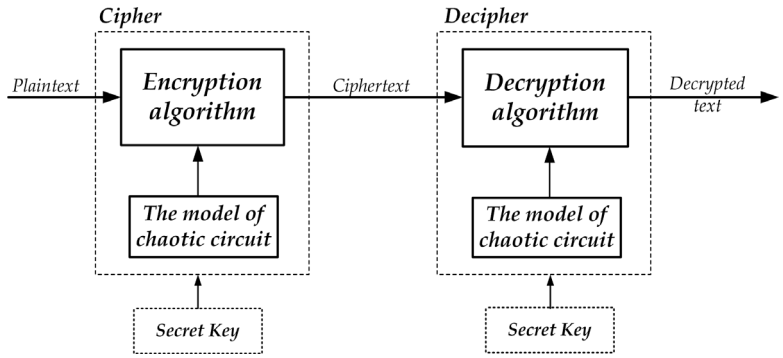


Fig. 12. The basic structure of a simple symmetric chaotic cryptosystem.

Like in the analog cryptosystem, also in the digital cryptosystem the chaotic circuit or its model is the basic component, performing the function of the random number generator. In analog cryptosystem these generators are analog circuits and they generate truly chaotic signals. In digital cryptosystem the generators are discrete systems which generate digital, pseudo chaotic signals.

According to the sort of the encryption algorithm the chaotic cryptosystem can be symmetric, stream or block and asymmetric. The secret key consists of the values of the parameters of the encryption function and/or the parameters of the pseudo random number generator.

Among the first patented symmetric chaotic cryptosystem were block as well as stream cryptosystem (Bianco & Reed, 1991; Gao, 1997). In stream ciphers, the encryption function is a simple logical operation XOR. A plaintext is ciphered by carrying out a logical XOR operation between the bits of the plaintext and the bits of the pseudo random sequence. The latter is generated on the basis of various algorithms (logistic equation, Lorenz's chaotic equations etc.) The ciphertext is deciphered with a XOR function of the ciphertext bits and the pseudo random sequence which equals the one used at ciphering (Fridrich, 1998).

In more recent chaotic cryptosystems the chaotic systems are incorporated into the encryption function in various ways. These systems are much more complex and also offer higher security. Their characteristics are perfectly comparable with the characteristics of the classical cryptosystems (Kocarev, 2001, Kocarev, & Lian, 2011).

4. The cryptosystem with the model of Chua's circuit

In this chapter a simple example of a chaotic cryptosystem, realized in the Matlab environment, is described. The model of the Chua's Circuit with a 5-scroll chaotic attractor discussed previously was used for generating pseudo random sequences; as the encryption algorithm a special multi-shift encryption function was used which is described in detail below.

4.1 The encryption function

The *N*-shift or the multi-shift encryption function can be described with the iterative algorithm described by the following equation (Yang et al. 1997, Šalamon & Dogša, 2002):

$$s(n) = \underbrace{f_1(\ldots f_1(f_1}_{N}(i(n), \underbrace{k(n)), k(n)), \ldots, k(n))}_{N}. \tag{9}$$

where N is the number of iterations, $i(n)$ the value of n-th sample of the plaintext, $k(n)$ is the n-th value of the chaotic variable, and f_1 is a non-linear function, described by the equation:

$$f_1(x,k) = \begin{cases} (x+k) + 2 \cdot h & -2 \cdot h \le (x+k) \le -h \\ (x+k) & -h < (x+k) < h \\ (x+k) - 2 \cdot h & h \le (x+k) \le 2 \cdot h \end{cases}. \tag{10}$$

Its graphic presentation is given in figure 13.

The encryption function will be bijective if the value of the variable h is chosen in the way that x and k will always be within the interval ($-h$, h):

$$-h < x < h \tag{11}$$

$$-h < k < h \tag{12}$$

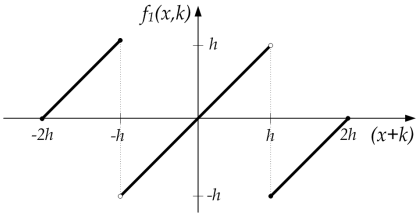


Fig. 13. The graph of non-linear function f_1.

In this case there is also the inverse – decryption algorithm described by the equation:

$$i(n) = \underbrace{f_1(...f_1(f_1}_{N}(s(n), \underbrace{-k(n)), -k(n)), ..., -k(n))}_{N} \tag{13}$$

where: $s(n)$ is n-th sample of the ciphertext and $i(n)$ is n-th sample of the decrypted text. f_1 is a non-linear function described by an equation (10). As the encryption and the decryption functions are recursive, a certain time is necessary to calculate the individual values of the ciphertext or the sample of the deciphered text. The time depends on the selected number of iterations N.

4.2 Details of the chaotic cryptosystem

Our cryptosystem belongs to the symmetric cryptosystems and can be used to cipher various kinds of plaintexts (text files, pictures, sound …) It is designed in the mathematical environment Matlab which enables flexible designing of prototypes and performing the cryptanalysis.

In this article a variant of a chaotic cryptosystem is described which has been adapted to ciphering and deciphering digital images. Its principal structure is shown in figure 14. The unit to be encrypted is represented by the pixel $i(n)$ on the image. The pixel is represented by three component intensities of primary colours: red $i_{red}(n)$, green $i_{green}(n)$ and blue $i_{blue}(n)$. Each component is represented by an 8-bit number.

Within a single encryption cycle all three components of an individual pixel are ciphered with three equal encryption functions. At the selected number of iterations of the encryption function N the cryptosystem ciphers the pixel $i(n)$ into pixel $s(n)$.

The pseudo random values are formed by three chaotic sate variables of the model of Chua's Circuit $x(n)$, $y(n)$ and $z(n)$. According to the necessary condition of inversion of the encryption and decryption algorithms, described by the equation (12), the state variables x, y and z are properly normalized.

The samples of the plaintext, ciphertext and the secret keys are values, represented by a number of bits in the digital cryptosystems. In the prototype realization of our cryptosystem, individual samples of the plaintext and random values $x(n)$, $y(n)$ and $z(n)$ were treated as double precision numbers, limited to the interval $(-h, h)$.

The secret key is composed of the values of the Chua's Circuit parameters: a, β, m_1-m_5, c_1-c_5, the initial values of the state variables $x(0)$, $y(0)$, $z(0)$ and the number of iterations N of the non-linear function f_1.

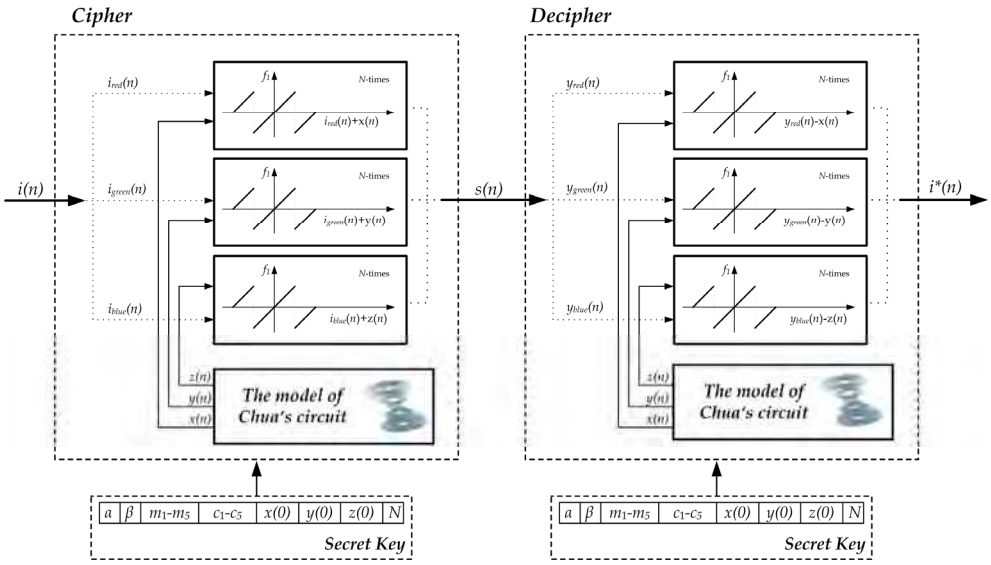


Fig. 14. The structure of the chaotic cryptosystem.

The encryption procedure is as follows: the random value *(x(n), y(n), z(n))* is added to the *n*-sample of a plaintext ($i_{red}(n)$, $i_{green}(n)$, $i_{blue}(n)$). After *N* iterations have been carried out, the *n*-sample of the ciphertext *s(n)* is generated by the function f_1. It is then transformed into the decrypted sample *i*(n)*, being only equal to the original sample *i(n)* if the key used at decryption equals the secret key used by encryption.

In cryptosystems the secret key is an optional value, represented by a definite number of bits. This is not valid for our cryptosystem as we have not ensured safe encryption with arbitrary values of its parameters. Safe encryption could only be ensured by providing automatic elimination or disabling of those circuit parameters where the circuit would not behave chaotically. In this article we did not deal with the automatic generation of suitable secret keys. The secret keys were adequate and carefully chosen values.

4.3 Cryptanalysis

We do not only wish to present the cryptographic features of our cryptosystem by cryptanalysis. Above all, we wish to present the problems which can be expected in systems of this kind.

In the cryptanalysis we have mostly kept to discussing some statistical characteristics. We have carried out the statistical analysis of ciphertexts, and on the basis of the statistical distribution of the ciphertext we made inferences as to their being random. We carried out an even more detailed analysis of the ciphertext with auto-covariance and cross-covariance, thus searching for possible correlation between ciphertexts and plaintexts as well as the correlation among various ciphertexts.

4.3.1 Statistical analysis of ciphertexts

In the statistical analysis of ciphertexts we mainly focused on the statistical distributions of their samples. The ciphertext samples must be uniformly distributed in order to be equally probable. In such case they will enable no conclusions about any kind of corresponding plaintext information.

In the following part of the article the cryptanalysis is presented where a digital image with dimensions 640x320, format JPG, shown in figure 15a, was used as the plaintext. As the random number generator we used the Chua's Circuit with the parameters: a=9, β=9.9, m_0=0.9/7, m_1=-3/7, m_2 =3.5/7, m_3=-2/7, m_4=4/7, m_5=-2.4/7, c_1=1, c_2=2.15, c_3=3.6, c_4=6.2, c_5=9 and the initial conditions: $x(0)$=0.5, $y(0)$=0, $z(0)$=0.

The figures 15b-d show encrypted images with corresponding histograms at different numbers of iteration of the encryption function N=1, N=10 and N=1000. It is evident from the figure 15b that uniformly distributed values of the ciphertext cannot be obtained at N=1. Encryption with N=1 is not secure enough. Obtained results are comparable to the results achieved by the analog chaotic masking technique.

As the number N increases, the distribution of the ciphertext approaches to the uniform distribution, thus showing the need for the highest possible number of iterations of the encryption function. A higher number of iterations mean a longer lasting encryption procedure, but it also ensures decreased statistic dependence between plaintext and ciphertexts.

The analysis of the ciphertext histograms does not enable a more detailed insight into the characteristics of the ciphertext patterns and their correlations with patterns of the corresponding plaintext. This is the reason why we proceeded with the cryptanalysis with correlational and covariance analysis, respectively.

4.3.2 Auto-covariance and cross-covariance analysis

For better understanding let us first observe some basic features of the auto-correlation and cross-correlation. The cross-correlation of M samples of the random sequence $x(n)$ and $y(n)$ is defined by the equation:

$$\varphi_{xy}(m)=\begin{cases}\sum_{n=0}^{M-m-1} x(n)\cdot y(n+m), & m\geq 0\\ \varphi_{yx}(-m), & m<0\end{cases}, \tag{14}$$

where n and m are arguments limited within intervals: $0\leq n\leq M$-1 and $-(M$-1$)\leq m\leq(M$-1). Auto-correlation is a special case of the cross-correlation, therefore it can be written on the basis of the equation (14):

$$\varphi_{xx}(m)=\begin{cases}\sum_{n=0}^{M-m-1} x(n)\cdot x(n+m), & m\geq 0\\ \varphi_{xx}(-m), & m<0\end{cases}. \tag{15}$$

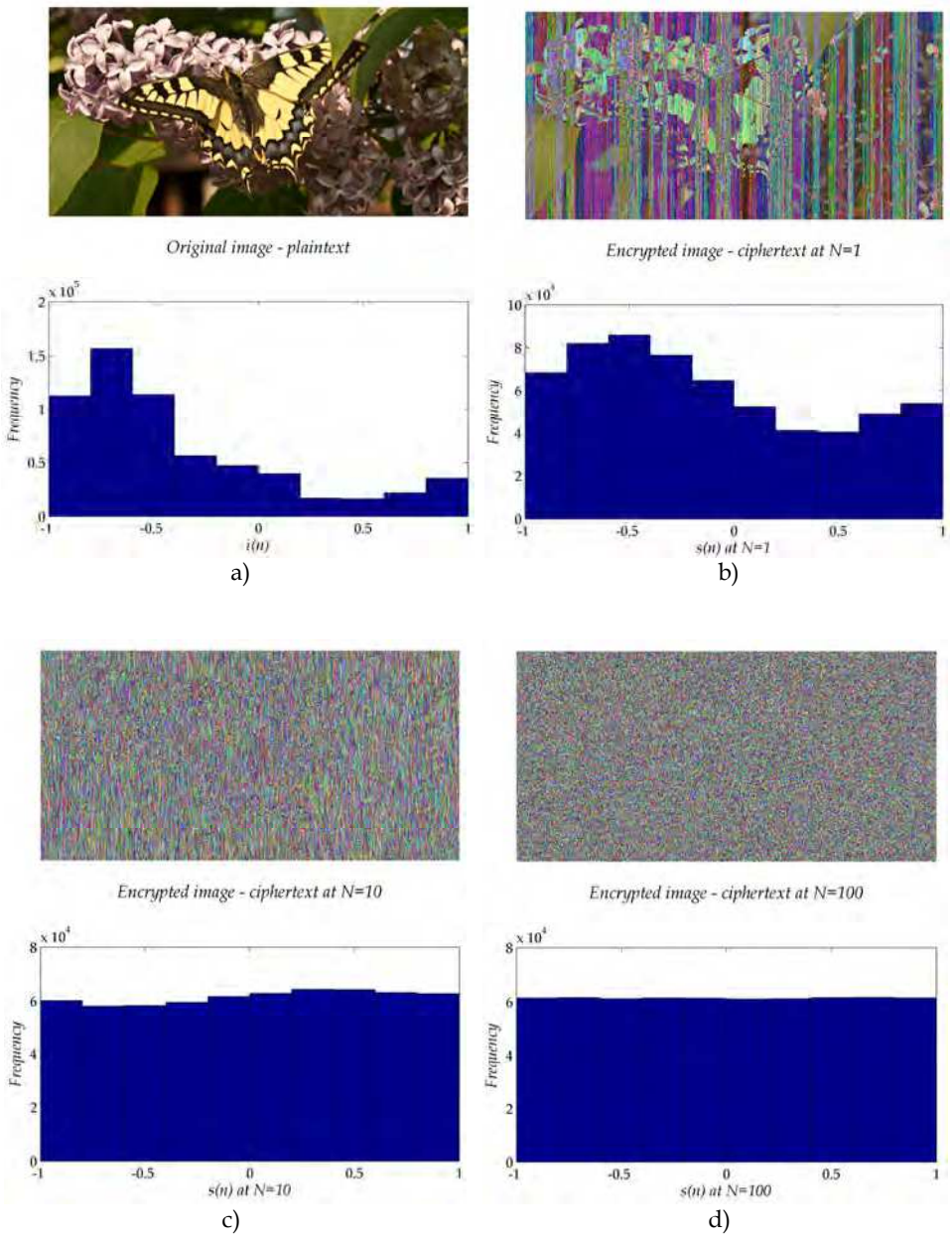


Fig. 15. a) Original image (plaintext) and its histogram. Encrypted images with the corresponding histograms at: b) N=1, c) N=10, d) N=100.

In the theory of probability and statistics covariance is also frequently used beside the correlation. The cross-covariance of the sequences *x(n)* and *y(n)* equals their cross-correlation if their mean value is eliminated from the sequences *x(n)* and *y(n)*. It is described by the following equation:

$$c_{xy}(m)=\begin{cases}\sum_{n=0}^{M-m-1}\left(x(n)-\frac{1}{M}\sum_{i=0}^{M-1}x_i\right)\cdot\left(y(n+m)-\frac{1}{M}\sum_{i=0}^{M-1}y_i\right), & m\geq 0\\ c_{yx}(-m), & m<0\end{cases}. \tag{16}$$

In the case of statistically completely independent sequences *x(n)* and *y(n)* the values of the cross-covariance for each argument *m* are equal zero. The more the sequences are correlated, the higher are the values of their cross-covariance.

The auto-covariance $c_{xx}(m)$ of the sequence *x(n)* is only a special case of the cross-covariance. Its features are as follows:

- if the sequence *x(n)* is periodical, its auto-covariance is also a periodical function $c_{xx}(m)$, retaining the period of the sequence *x(n)*;
- if the sequence *x(n)* is random, its auto-covariance is an even function $c_{xx}(m)=c_{xx}(-m)$ and has the following characteristics: at the argument $m=0$ it has its maximum, at an infinite argument it equals zero $c_{xx}(\pm\infty) = 0$, which means that »the beginning« and »the end« of the random function *x(n)* are statistically independent or non-correlated. There is no causal relationship between them or, »the end« of the sequence does not remember its »beginning«.

In cryptography the characteristics of the auto-covariance and cross-covariance can be used for a more detailed analysis of the ciphertext and their dependence of plaintext. In this way we can also make conclusions about the security which can be provided by an encryption system.

In the figure 16 the results of the covariance analysis with three different numbers of iterations of the encryption function $N=1$, $N=10$ and $N=100$ are shown. The blue graphs represent the auto-covariance of the ciphertexts, shown in figures 15b-d, the red graphs represent the cross-covariance of the same ciphertexts with the plaintext shown in figure 15a.

The auto-covariance of the ciphertexts obtained by encryption of the same plaintext at different numbers of iterations of the encryption function show that the ciphertexts are the more statistically independent the higher is the number of iterations. On the other hand, the cross-covariance of the ciphertext and the corresponding plaintext show that at $N=1$ we are dealing with a slightly emphasized statistical dependence of the original and encrypted image which decreases with the increasing number of iterations. At $N=10$ and $N=100$ the cross-covariance is very close to the zero value.

In the following part of the cryptanalysis we analysed the dependence of the statistical characteristics of ciphertexts on the secret key. Namely, the encryption system must ensure independence and insensitivity of the ciphertext to the selected secret key.

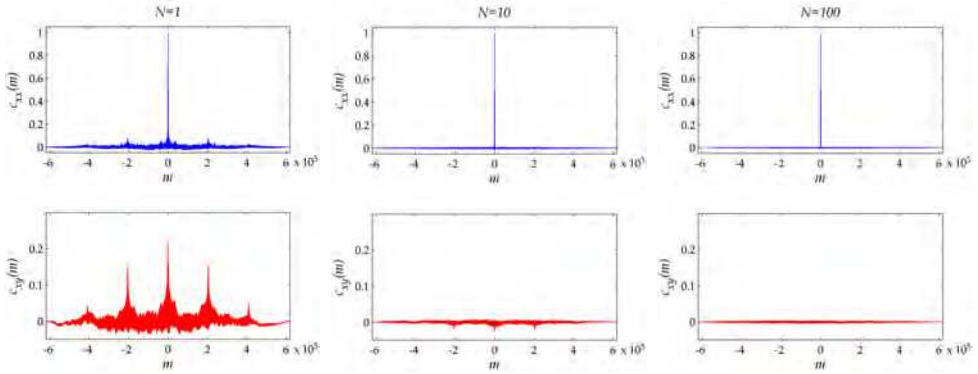
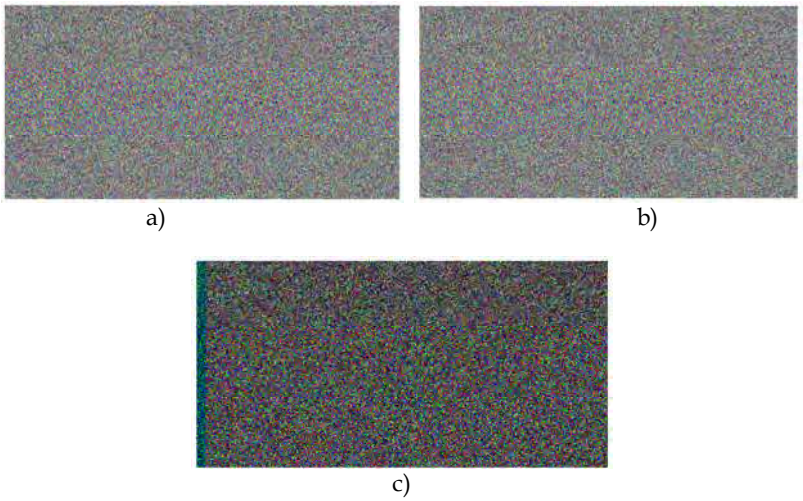


Fig. 16. Normalized auto-covariance $c_{xx}(m)$ of the ciphertexts, shown in figures 15b-d and their cross-covariance $c_{xy}(m)$ with the plaintext shown in figure 15a, at different numbers of iterations of the encryption function N=1, N=10 and N=100.

Example 1

We have analysed the differences between two ciphertexts A and B, obtained at the encryption of the same plaintext (figure 15a) with two very similar secret keys. They only differed from each other in the initial state of the chaotic state variable y. The initial state in the case of the ciphertext A was: $x(0)$=0.5, $y(0)$=0, $z(0)$=0, in the case of the ciphertext B it was: $x(0)$=0.5, $y(0)$=10^{-12}, $z(0)$=0. The rest of the secret key parameters were the same in both cases: a=9, β=9.9, m_0=0.9/7, m_1=-3/7, m_2 =3.5/7, m_3=-2/7, m_4=4/7, m_5=-2.4/7, c_1=1, c_2=2.15, c_3=3.6, c_4=6.2, c_5=9, N=100.

Figure 17 illustrates the results of the encryption: ciphertext A (figure 17a), ciphertext B (figure 17b) and the difference between them (figure 17c).



a) b)

c)

Fig. 17. a) Ciphertext A at $y(0)$=0; b) Ciphertext B at $y(0)$= 10^{-12}; c) The difference between the ciphertexts A and B.

The difference between ciphertext A and B is practically imperceptible. In spite of this, the figure 17c showing the difference between both images, enables us to see an exposed area. The reason for this area is a very small initial difference between the pseudo-random sequences which do not start to diverge more quickly till after a certain time and several generated values, respectively.

Although the behaviour of the Chua's Circuit is very sensitive to the change of the initial conditions, the chaotic sequences begin to diverge noticeably only after several thousand samples which is clearly shown in figure 18.

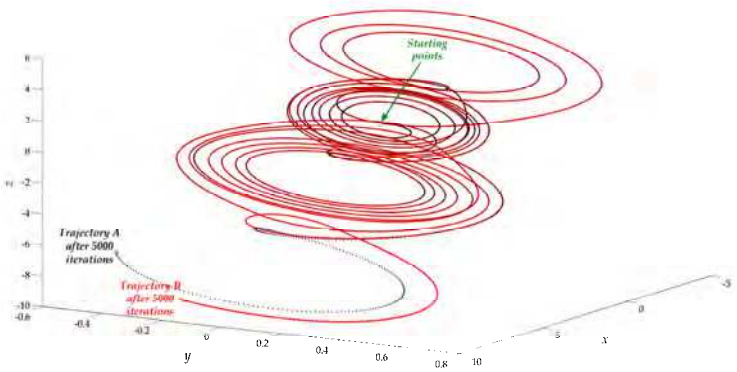


Fig. 18. Sensitivity to the initial conditions in the case of the trajectories A and B.

The figure shows the trajectories A and B in the state space, which start very close together and diverge from each other considerably after a certain time. This is the reason why the initial several thousand samples of the ciphertext A and B are very similar (black dots in image 17c). As the divergence of the trajectories depends on the size of the Lyapunov exponent value, we wish it to be as large as possible.

Example 2

In this case the encryption was carried out in the same way as in the example 1, but we left out the initial 20000 samples of the chaotic state variables. Thus we ensured a large divergence of the trajectories A and B at the very beginning of the encryption. The results are shown in figure 19.

Fig. 19. The difference between the ciphertexts A and B. The initial 20000 samples of random sequences, generated with a model of the Chua's Circuit, were left out.

The difference between the ciphertexts A and B (figure 19) shows that the similarity area of the ciphertexts, which was evident before, has disappeared. This can be more accurately evaluated with a cross-covariance of both ciphertexts. For the purpose of comparison figure 20 shows the cross-covariance of the ciphertexts A and B for both examples described above.

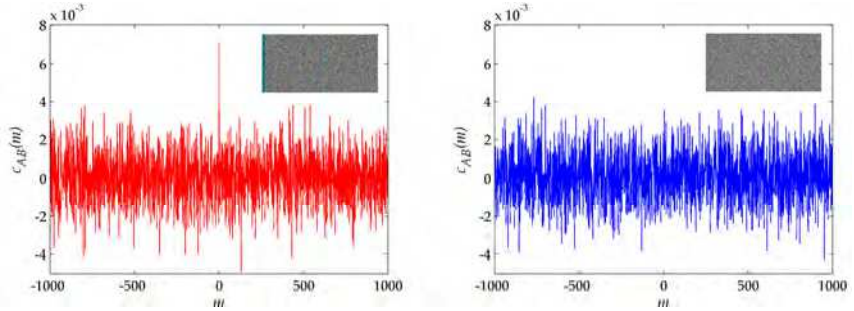


Fig. 20. Cross-covariance of the ciphertexts from examples 1 and 2, respectively.

In the first example (red graph) the aberrated cross-covariance value at the argument m=0 is noticeable, proving the initial correlativity of the compared ciphertexts. This is the consequence of the fact that the initial divergence of the pseudo-random sequences used was too slow. In the second example (blue graph) we do not notice any evident correlativity of the ciphertexts A and B, as the initial 20000 very similar or even equal samples of pseudo-random sequences were left out before the beginning of the encryption.

5. Conclusion

Chaotic electronic circuits generate chaotic, non-periodic signals. With an appropriate correction they can be modified into truly random signals, useful in cryptography. In the article we present the alternative for the random number generation with the chaotic Chua's circuit. We found out, that the basic variant of the Chua's circuit is not able to generate uniformly distributed random signals. Equally applies also for the modified Chua's circuit with 3-, 4-, 5-scroll chaotic attractors. Lyapunov exponent analysis points out that a sensitivity of the Chua's circuit to initial conditions increases with the complexity of chaotic attractors.

If the initial conditions of chaotic state variables represent the parts of secret key, in a cryptographic sense, a sensitivity to initial conditions should be as large as possible. Therefore, we have chosen for the random number generator, the variant of Chua's circuit with 5-scroll chaotic attractors. With the digital model of this circuit and the appropriate recursive function we have designed the cryptographic system adapted for a digital images encryption. For an individual image pixel encryption we have used three available chaotic state variables. Theirs uniform distribution was assured with the additional recursive function used for an encryption. The secret key could not be an arbitrary value but an adequate and a carefully chosen value consisting of the Chua's circuit parameters, initial conditions and a number of encryption function iterations. Namely, the bifurcation diagrams and Lyapunov exponents show that the Chua's circuit only behaves chaotically at certain values of components and parameters.

From a cryptographic point of view uniformly distributed ciphertexts are always required. In our crypto system, we could satisfy this requirement only by using an additional recursive function with a large enough number of its iterations. In such cases, the auto-covariance of ciphertexts was always very close or equal to the zero value. Similar conclusions were reached also in the ciphertexts cross-covariance analysis with the corresponding plaintexts. Statistical independence of ciphertext and plaintext samples was assured only with a large enough number of encryption iterations.

One of the essential properties of all chaotic systems is a high sensitivity to initial conditions and some parameters. Despite of the infinitesimal small deviation of two initial conditions, the Chua's circuit generates signals with several thousand very similar initial time-values. This is obviously undesirable, since each of so small secret key changes, should be reflected with a very large ciphertext change. Thus, the problem of ciphertexts initial similarity appears by encryption with the very similar secret keys. In our case, we have analysed this problem with a cross-covariance of ciphertexts. By elimination of the initial 20000 chaotic values the problem was completely resolved.

In the paper, we have pointed out the problems that may occur when the chaotic circuits are using in the cryptographic systems. Described problems can be avoided by appropriate automatic secret keys generation, which requires precise knowledge of the chaotic circuit behaviour and the properties of encryption function.

Automatic secret keys generation for a chaotic cryptographic system can be a challenge for a further research work that links two interesting areas: deterministic chaos and cryptography.

6. References

Bianco, M. E. & Reed, D. A. (1991). *Encryption system based on chaos theory*. US Patent No. 5048086, (September 1991), USA

Chua, L. O.; Komuro, M. & Matsumoto, T. (1986). The double scroll family. *IEEE Transactions on Circuits and Systems*, Vol.33, No.11, (November 1986), pp. 1072-1118, ISSN 0098-4094

Chua, L. O.; Wu, C. W.; Huang, A. & Zhong (1993). A universal circuit for studying and generating chaos. I. Routes to chaos. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, Vol.40, No.10, (October 1993), pp. 732-744, ISSN 1057-7122

Corron, N. J. & Hahs D. W. (1997). A new approach to communications using chaotic signals. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, Vol.44, No.5, (May 1997), pp. 373-382, ISSN 1057-7122

Cuomo, K. M.; Oppenheim, A. V. & Strogatz, S. H. (1993). Synchronization of Lorenz-based chaotic circuits with applications to communications. *IEEE Transactions on Circuits and Systems-II: Analog and Digital Signal Processing*, Vol.40, No.10, (October 1993), pp. 626-633, ISSN 1057-7130

Dedieu, H.; Kennedy, M. & Hasler, M. (1993). Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits. *IEEE Transactions on Circuits and Systems-II: Analog and Digital Signal Processing*, Vol.40, No.10, (October 1993), pp. 634-642, ISSN 1057-7130

Fortuna, L.; Frasca, M. & Xibilia, M. G. (2009). *Chua's Circuit Implementations – Yesterday, Today and Tomorrow*. World Scientific Publishing Co. Pte. Ltd., ISBN-13 978-981-283-924-4, Danvers, USA

Fridrich, J. (1998). Symmetric Ciphers Based on Two-Dimensional Chaotic Maps. *International Journal of Bifurcation and Chaos*, Vol.8, No.6, (June 1998), pp. 1259-1284, ISSN 0218-1274

Gao, Z. (1997). *Method and apparatus for encrypting and decrypting information using a digital chaos signal*. US Patent No. 5696826, (December 1997), USA

Hilborn, R. C. (2000). *Chaos and Nonlinear Dynamics, An Introduction for Scientists and Engineers, Second Edition*, Oxford University Press, ISBN 0198507232, New York, USA

Hongtao, L. & Zhenya, H. (1996). Chaotic Behavior in First-Order Autonomous Continuous-Time Systems with Delay. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, Vol.43, No.8, (August 1996), pp. 700-702, ISSN 1057-7122

Kennedy, M. P. (1993). Three steps to chaos. I. Evolution. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, Vol.40, No.10, (October 1993), pp. 640-656, ISSN 1057-7122

Kennedy, M. P. (1993). Three steps to chaos. II. A Chua's circuit primer. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, Vol.40, No.10, (October 1993), pp. 657-674, ISSN 1057-7122

Kennedy, M. P. (1994). Chaos in the Colpitts oscillator. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, Vol.41, No.11, (November 1994), pp. 771-774, ISSN 1057-7122

Kocarev, L. (2001). Chaos-based cryptography: a brief overview. *IEEE Circuits and System Magazine*, Vol.1, No.3, (Third Quarter 2001), pp. 6-21, ISSN 1531-636X

Kocarev, L. & Lian, S. (2011). *Chaos-Based Cryptography Theory, Algorithms and Applications*. Springer-Verlag, ISBN 978-3-642-20541-5, Berlin, Germany

Koh, C. L. & Ushio, T. (1997). Digital communication method based on M-synchronized chaotic systems. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, Vol.44, No.5, (May 1997), pp. 383-390, ISSN 1057-7122

Kolumban, G. & Vizvari, B. (1994). Nonlinear dynamics and chaotic behavior of the sampling phase-locked loop. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, Vol.41, No.4, (April 1994), pp. 333-337, ISSN 1057-7122

Ogorzalek, M. J. (1993). Taming chaos. I. Synchronization. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, Vol.40, No.10, (October 1993), pp. 693-699, ISSN 1057-7122

Ogorzalek, M. J. (1997). *Chaos and complexity in nonlinear electronic circuits*. World Scientific Publishing Co. Pte. Ltd., ISBN 981-02-2873-2, Danvers, USA

Schneier, B. (1996). *Applied cryptography: protocols, algorithms, and source code in C*. John Wiley and Sons, ISBN 0471128457, Canada

Sharkovsky, A. N. & Chua, L. O. (1993). Chaos in some 1-D discontinuous maps that appear in the analysis of electrical circuits. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, Vol.40, No.10, (October 1993), pp. 722-731, ISSN 1057-7122

Sprott, J. C. (2009). *Chaos and Time-Series Analysis*. Oxford University Press, ISBN 978-0-19-850839-7, New York, USA

Stallings, W. (1999). *Cryptography and Network Security Principles and Practice, Second Edition*. Prentice-Hall, ISBN 0138690170, Upper Saddle River, New Jersey USA

Suykens, J. A. K. & Vandewalle, J. (1993). Generation of n-Double Scrolls (n = 1, 2, 3, 4, …). *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, Vol.40, No.11, (November 1993), pp. 861-867, ISSN 1057-7122

Šalamon, M. & Dogša, T. (1995). Analysis of chaos in the Chua's oscillator. *Electrotechnical review: journal of electrical engineering and computer science,* Vol.62, No.1, (October 1995), pp. 50-58, ISSN 0013-5852

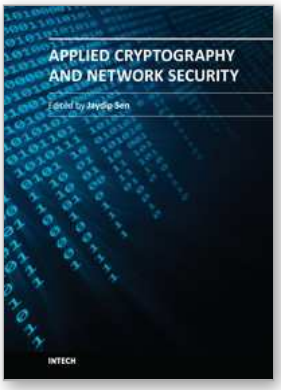
Šalamon, M. & Dogša, T. (2000). Danger of Chaos in a second-order Digital Filter. *Informacije MIDEM - Journal of microelectronics, electronic components and materials*, Vol.30, No.1, (March 2000), pp. 37-42, ISSN 0352-9045

Šalamon, M. & Dogša, T. (2002). A comparative analysis of chaotic encryption systems with the XOR encryption function and multishift encryption function. *Electrotechnical review: journal of electrical engineering and computer science*, Vol.69, No.2, (June 2002), pp. 107-112, ISSN 0013-5852

Šalamon, M. & Dogša, T. (2009). The model of chaoticness detector. *Informacije MIDEM - Journal of microelectronics, electronic components and materials*, Vol.39, No.2, (June 2009), pp. 93-99, ISSN 0352-9045

Yang, T. & Chua, L. O. (1996). Secure communication via chaotic parameter modulation. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, Vol.43, No.9, (May 1997), pp. 817-819, ISSN 1057-7122

Yang, T.; Chai, W. W. & Chua, L. O. (1997). Cryptography based on chaotic systems. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, Vol.44, No.5, (May 1997), pp. 469 - 472, ISSN 1057-7122



Applied Cryptography and Network Security
Edited by Dr. Jaydip Sen

ISBN 978-953-51-0218-2
Hard cover, 376 pages
Publisher InTech
Published online 14, March, 2012
Published in print edition March, 2012

Cryptography will continue to play important roles in developing of new security solutions which will be in great demand with the advent of high-speed next-generation communication systems and networks. This book discusses some of the critical security challenges faced by today's computing world and provides insights to possible mechanisms to defend against these attacks. The book contains sixteen chapters which deal with security and privacy issues in computing and communication networks, quantum cryptography and the evolutionary concepts of cryptography and their applications like chaos-based cryptography and DNA cryptography. It will be useful for researchers, engineers, graduate and doctoral students working in cryptography and security related areas. It will also be useful for faculty members of graduate schools and universities.

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821