Bulletin of the *Transilvania* University of Braşov • Vol 2(51) - 2009
Series III: Mathematics, Informatics, Physics, 113-126

CHAOS-BASED CRYPTOGRAPHY. A POSSIBLE SOLUTION FOR INFORMATION SECURITY

Cristian-Iulian RÎNCU [1] **and Alexandru ŞERBĂNESCU** [1]

Communicated to:
9-ème Colloque franco-roumain de math. appl., 28 août-2 sept. 2008, Braşov, Romania

Abstract

The development of the new information security systems based on chaos theory represents a new research field in communication and information technology domain. Cryptography is a permanent field of interest at all times. At present secret communication plays an increasing role in many fields of common life, like banking, industry, and telecommunication. In this paper we present some aspects regarding the chaos-based cryptography stage. The essence of the theoretical and practical efforts which are done in this new field is represented by the idea that chaos-based cryptosystem is capable to have similar performances regarding the classic methods based on computational techniques. We show that some of these performances are obtained using several well-known chaotic ciphers.

1. Introduction

Modern telecommunication networks, and especially the Internet and mobile-phones networks, have tremendously extended the limits and possibilities of communications and information transmissions. Associated with this rapid development, there is a growing demand of cryptographic techniques, which has spurred a great deal of intensive research activities in study of cryptography. The techniques of secure communications by which one can transmit confidential messages secretively are of practical interest in several areas, including databases, internet banking, software, protection of communication channels. The need of communication and the rapid increase of the amount of the information transmitted using network communications have determined the development of new secure techniques to protect the information. Cryptography is the best solution against the unauthorized use of the information. In the last years, researchers have remarked the similarities between chaos and cryptography[6, 2]. Several of the dynamical chaotic system features can be correlated with the cryptographic properties.

[1]Military Technical Academy, Romania

2. Dynamical Chaotic Systems

It is very difficult to formulate a definition of chaos that is universal. Paradigms of chaos are intended to convey intuitively how very complex behavior can arise in nature. While chaos is the study of how simple systems can generate complicated behavior, complexity is the study of how complicated systems can generate simple behavior. Complex systems are spatially and/or temporally extended nonlinear systems characterized by collective properties associated with the system as a whole and that are different from the characteristic behaviors of constituent parts. A dynamical system consists of an abstract phase space (or state space), whose coordinates describe the dynamical rule which specifies the immediate future trend of all state variable, given only the present value of those same state variables. A dynamical system can have discrete or continuous time evolution. A map defines the discrete case $z_{n+1} = f(z_n)$ that gives the state z_{n+1} resulting from the state z_n at the next time value. A deterministic system is perfectly predictable given perfect knowledge of the initial conditions and it is in practice always predictable in the short term. Chaos is an effectively unpredictable long time behavior arising in a deterministic dynamical system because of sensitivity to initial conditions. Chaos is a particular state of a nonlinear dynamical system and appears only in certain conditions, e.g. for certain values of the system parameters. The chaotic state can be observed in a first approach by the existence in the phase space of a chaotic attractor or fractal in which all the system trajectories evolve following a certain pattern (basin of attraction) but are never the same. In a more analytical approach, the chaotic state can be very well studied by the Lyapunov exponents, which globally characterize the behavior of a dynamical system. Chaos will be observed only when there is at least one positive Lyapunov exponent and the total sum of all exponents is negative, that is the dynamical system has a stable but random like state called chaotic state. The highly unpredictable and random-look of chaotic signals is the most attractive feature of deterministic chaotic systems that may lead to novel engineering applications.

3. Chaos and Cryptography

Telecommunications technology continues to advance with great pace and momentum and as technology expands, as do the threats to those communications. There is a seemingly eternal battletaking place between those who wish to protect their communications lines and those who wish to invade them. Between the cryptographer and cryptanalyst and between the security manager and the intruder, as each side seeks to gain the initiative over the other. The problem of finding secure communications methods, which transmit confidential information secretively, has a practical interest in several areas, including the protection of communication channels, databases, and software. In the last decade the science proved the existence of the possibility to realize the digital communication system with the non-linear devices and electronic circuits. This behavior of the circuits was named chaotic because it was discovered the randomness generated by these simple systems that are very sensitive to their initial conditions. That's way if two chaotic systems almost identical have two initials states with a very little different the behavior of the two

systems will diverge very fast. The development of the new information security systems based on dynamical chaotic systems represents a new research field in communication and information technology domain. There are a lot of papers on this subject but it takes long time to validate such a new proposed system. The essence of the theoretical and practical efforts which are done in this new field is represented by the idea that chaos-based cryptosystems are capable to have similar performances as the classical methods based on computational techniques. The cryptography is as old as the need of sending confidential messages for long distances and protected stored data. Now, in the time of computer global communication and mobile telephony, there is a necessity of creating new, but fast and secure algorithms for encryption and decryption. The growth of electronic commerce and the emphasis of privacy have intensified the need to find a fast and secure cryptographic method. In general, there are two types of cryptographic schemes: public-key and private-key schemes. Cryptography with chaos falls into the category of private-key schemes, that the same secret key is used for both encryption and decryption. This cryptographic approach relies on the properties that chaotic signals are usually noise-like and chaotic systems are very sensitive to initial condition. Therefore the secret keys usually contain the system parameters and the initial condition. Many researchers have point out that there exist tight relationship between chaos and cryptography[6, 2, **?**]. Many fundamental characteristics of chaos, such as ergodicity, mixing and property of the sensitivity to initial conditions can be connected with the confusion and diffusion property in cryptography. So it is a natural idea to use chaos to enrich the design of new ciphers. Among the most promising applications of chaotic systems is their use in the field of chaotic encryption where the utilization of nonlinearities and the constraining of the dynamical system to a chaotic state will fulfill in our opinion the basic cryptographic requirements. Due to the nonlinear mechanisms that lead to a chaotic behavior, this one is too difficult to be predicted by analytical methods without the secret key (initial conditions and/or parameters) being known. This would reduce a potential attack to one category - that of a brute force attack, in which any attempt to crack the key depends directly upon how long (or complicated) the key is. In the recent years there are a lot of international studies center which are interested in solving the problem of the proper using of the nonlinear dynamical systems with chaotic behavior in secure communication scheme. The basic ideas can be classified into three major types: individual data channel encryption, multiplexed data channel encryption and their combining form.

The relationship between the chaotic systems and cryptosystems is straightforward because a good cryptosystem (based on symmetric or asymmetric encryption) should:

- be sensitive with respect to keys: flipping one bit in a key creates completely different ciphertext when applied to the same plaintext;
- be sensitive with respect to plaintext: flipping one bit in the plaintext creates completely different ciphertext;
- map plaintext to random ciphertext: there should not be any patterns in the ciphertext, if the cryptosystem is good.

The chaotic systems have the following properties:

- parameter sensitivity: small variation in one of the system parameters is enough to make two trajectories, starting from the same initial point, separate at exponential rate;
- initial condition sensitivity: two trajectories starting from two different, though arbitrarily close, initial points separate from each other exponentially;
- ergodicity: the trajectories followed by points belonging to the phase space travel through the space with uniform distribution.

Classic cryptography works with discrete values and in discrete time while the crucial point in chaotic cryptography is the usage of continuous-value systems that may operate in continuous or discrete time. As a result, in order to ensure an appropriate design and analysis methods for chaotic cryptographic systems, some special considerations must be taken into account. Chaotic maps and cryptographic algorithms (or more generally maps defined on finite fields) have also some similar properties: sensitivity to initial conditions and parameters, random like behavior and unstable orbits with long periods, depending upon the precision of the numerical implementation. Encryption rounds of a cryptographic algorithm lead to the desired diffusion and confusion properties of the algorithm. In a similar manner, iterations of the chaotic map spread the initial region over the entire phase space while the parameters of the chaotic map may represent the key of the encryption algorithm. An important difference between chaos and cryptography is the fact that the encryption transformations are defined on finite fields, while chaos has meaning only on real numbers. On the other hand, an extension of the domain of a classic encryption algorithm from a finite to a continuous field will give rise to a chaotic map. Until now chaos was successfully implemented in analog secure systems following the works of Pecora and Carroll in 1990 [15]. However, implementations in digital systems have not yet been successfully. The major reason why digital cryptography using chaos did not turn out to be effective is that digital circuits deal with finite number spaces. Chaos is a phenomenon in which every very small variation in the initial state of a system results in exponentially diverging evolution of its future states. When dealing with finite number space, chaos looses this diversity due to the restricted resolution of possible states [2].
As a result of investigating the relationship between chaos and cryptography, a rich variety of chaos-based cryptosystems for end-to-end communications has been put forward. There are two possibilities to achieve information security systems based on dynamical chaotic components: analog and digital.

4. Chaos-based Cryptography

4.1. Analog chaos-based communication systems

The majority of the analog chaos-based cryptosystems are secure communication schemes designed for noisy channels. They are based on the technique of chaos synchronization. Chaos synchronization is a technique developed since 1990s [15]. Theoretically, these systems used to protect the information are based on the idea that two chaotic systems can

synchronize with each other under the driving of one or more scalar signals, which are generally sent from one system to another [2]. There are many different types of chaos synchronization, such as: complete synchronization, generalized synchronization, impulsive synchronization, phase synchronization, projective synchronization, lag synchronization, noise-induced synchronization, depending on the different mathematical definitions of the chaos synchronization [1]. In analog chaotic cryptosystems, the information can be transmitted by one or more chaotic signals in a number of ways, including the following ones:

- chaotic masking. In this case, the analog message signal $m(t)$ is added to the output of the chaos generator, $x(t)$, within the transmitter [7, 14];
- chaotic switching or chaos shift keying (CSK), in which, a binary message signal is used to choose the carrier signal from two or more different chaotic attractors;
- chaotic modulation. In this situation, the message modulates a parameter of the chaotic generator or, when spread spectrum techniques are used, the message signal is multiplied by the chaotic carrier signal [4];
- chaos control method. In this case, small perturbations cause symbolic dynamics of a chaotic system to track a prescribed symbol sequence;
- inverse system approach, in which, the receiver system is designed in an inverse manner to ensure the recovery of the encryption signal [1];

Regardless of the method used to transmit the message signal, the receiver has to synchronize with the transmitter's chaotic generator so as to regenerate the chaotic carrier signal $x(t)$ thereby recovering the message via signal separation.

4.2. Digital ciphers

As compared to the analogic cryptosystems, digital chaos-based ones (also called digital chaotic ciphers), are designed for digital processors, where there are one/more chaotic maps implemented in finite computing precision in order to encrypt the plain-message in a number of ways, such as the following ones:

- stream ciphers based on chaos-based PRNGs (pseudo-random number generators). As a consequence that the chaotic systems can generate unpredictable pseudo-random orbits, many cryptosystems have been developed using chaos based PRNGs. Many chaotic pseudo-random sequences have been proved to have perfect statistical properties for continuous-values chaotic systems. The kernels of most chaotic stream ciphers are chaotic PRNGs, whose outputs are the key streams used to mask (generally using an XOR operation) the plain-texts [9, 8];
- chaotic stream ciphers via inverse system approach (with cipher text feedback). Generally speaking, chaotic inverse system approach actually restates the basic encryption model of a general cipher, so it can be used in both analog and digital

situations, and either in stream ciphers or block ciphers. Regarding these systems, the plaintext is not mainly encrypted by chaotic system, but by a key stream generated by chaotic systems with cipher-texts feedback. These chaotic systems can be also based on a one-way couple map lattices serving as chaotic systems, multiple maps being simultaneously used for encryption and decryption [11];

- block ciphers based on forward/backward chaotic iterations. These chaotic ciphers have been proposed mainly as image encryption methods. The ciphers can be based on 2-D chaotic maps. The basic procedure of these ciphers iterates a 2-D map to pseudo-randomly permutes the pixels in plain-image, uses some substitution algorithm to flatten the histogram of plain-image and repeats these procedures for n times to obtain cipher-image. The ciphers can be based also on two different cascaded chaotic systems. To ensure the correctness of decrypted data, the periods of both chaotic orbits should be fixed [12];

- chaotic ciphers based on searching plain-bits in a chaotic pseudo-random sequence. Because of their special design is rather difficult to classify these ciphers into stream or block ciphers. The pseudo-random sequence is the chaotic orbit itself. The encryption procedure uses the iteration of the chaotic system until the orbit arrives in the unit representing the plain-text and records the number of chaotic iterations as the cipher text [3];

- block ciphers based on chaotic round function or S-boxes. Taking into account other ideas regarding digital chaotic ciphers, we may consider that S-boxes generated via digital chaos can be a more promising and essential way to connect chaos with conventional cryptography. There are two classes of S-boxes generated from chaos: dynamic S-boxes and fixed S-boxes [16, 17].

The above mentioned ciphers do not depend on chaos synchronization, but they usually use one or more chaotic maps instead of that. The initial conditions and the control parameters play the role of the secret key. The information security systems can also be used to achieve others security services like authentication and data integrity [17, 18].

5. Chaos-Based Ciphers

5.1. Baptista method

An interesting new idea to develop chaotic ciphers was proposed in 1998 by Baptista [3]. This simple and easy to be understood method is based on the use of a well-known digital chaotic map, logistic function, that is defined using the expression:

$$F : X \to X, \;\; F(x) = rx(1-x) \tag{1}$$

where r is the parameter of logistic map that determines the chaotic behaviour, with $x \in (0,1)$ and $3.57 \leq r \leq 4$ for good chaotic properties. The value of r parameter is very important because only for the some area of the domain presented above, the logistic map

has a good chaotic behaviour and this thing can be seen in bifurcation diagram (figure 1) that help us to find the proper chaotic area. The principle of obtaining the bifurcation diagram is to vary just one parameter (which is r in the case of logistic map). This diagram shows each potential state at every value of r. Each state is represented by a point on the bifurcation diagram.

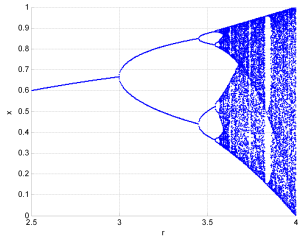

Figure 1: Bifurcation diagram for logistic map

Using the bifurcation diagram we can distinguish three areas that represent distinctive states for the logistic map. For some values of r, the system has just one state, while for other values it has two or more states but not enough for a good chaotic behaviour recommended for an use in cryptosystems. There are only some regions which can assure a real chaotic behaviour for the logistic map. We have used the value 3.996 in our simulations, for example. The algorithm presented by Baptista has the following principle. For the logistic function defined using formula (1), we can choose a domain $X = [x_{min}, x_{max}] \subset [0, 1]$ and split it in equal length sites (with length $\varepsilon = \frac{x_{max} - x_{min}}{S}$) for every alphabet letter like is presented in the figure 2.

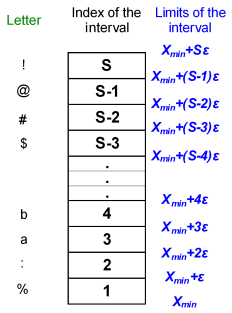

Figure 2: The domain of logistic map that is used by the algorithm

The encryption process can be described using the following steps:

- for every plain-character m_i, the process iterates the chaotic system from the initial condition x_0 to find a chaotic state x that is included in the right character site;
- the iteration number C_i of the function is recorded as the first possible cipher-message unit if another condition is satisfied. That cipher-message unit C_i should be constrained by $N_{min} \leq C_i \leq N_{max}$ ($N_{min} = 250$ and $N_{max} = 65532$). More than, an extra coefficient $\eta \in [0, 1]$, is used to choose the right value of possible number of iterations. A pseudo-random number k (with a normal distribution within the interval [0, 1]) is generated when a new right value C_i is found and if it is satisfied the condition $k \geq \eta$ this number C_i is the right ciphertext unit.

The decryption process uses the following steps:

- for each ciphertext unit C_i, we need to iterate the same chaotic system for C_i times from the last state x_0 and then use $x = F^{C_i}(x_0)$;
- find the plain-character m_i using the association map presented above which is a part of the private key.

There are many drawbacks of Baptista approach [5, 10], but one of them is that the cryptographic scheme is too slow. For this reason we can reduce the number of entries so that the desired region can be reached at a smaller number of iterations. To maintain a good level of security and to obtain in the same time confidentiality and another security services (authentication, data integrity), Wong proposed a chaotic cryptosystem using a dynamic look-up table instead of a static one [19] and after that combines the chaotic cryptographic with a hashing scheme [18]. Consequently, the relationship between consecutive cipher-text becomes dynamic and it is more difficult to break it, and there are accomplished another security services. Using this algorithm the cryptosystem can perform both encryption and the hashing to produce the cipher text as well as the hash value for a given message [17]. In this manner can be achieved both authentication added to confidentiality.

5.2. A discrete chaotic cryptosystem using external key

This cryptographic system is a symmetric key block cipher using the essence of chaos. Unlike the presented above chaotic cryptosystem which uses the parameter and the initial condition of the chaotic map as the key, this cryptosystem uses an external key of variable length to generate both the parameter and the initial condition for the chaotic map. The encryption of each block of plaintext is dependent on the secret key and, in this way the cryptosystem becomes stronger against any reasonable attack that uses feedback techniques [20].
The cipher uses the same logistic map (1) as a dynamical system. The secret key of the system is an external key and is on 128 bits in our explanation. The key $K = K_1K_2 \dots K_{16}$ for encryption/decryption process will be divided in blocks of 8-bits named session keys.

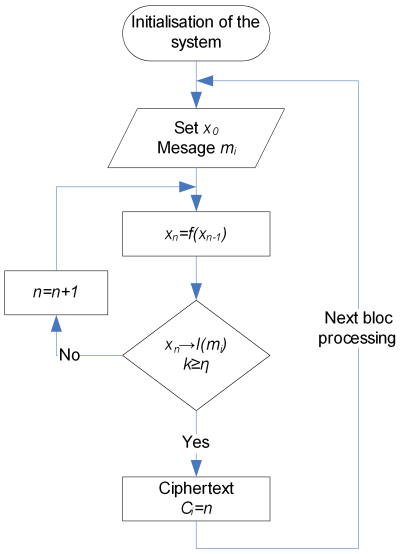

Figure 3: Baptista encryption algorithm

The values of the initial condition and of the parameter for the logistic chaotic map are generated on the bases of the secret key using the next formulas:

$$X_s = \frac{((K_1)_2 \oplus (K_2)_2 \oplus \ldots (K_{16})_2)_{10}}{256} \tag{2}$$

$$N_s = K_1 + K_2 + \ldots + K_{16} \tag{3}$$

For every new encrypted or decrypted character the values obtained above are modified using one part of the key that is randomly chosen:

$$X = \left(X_s + \frac{K_r}{256}\right) mod 1 \tag{4}$$

$$N = N_s + K_r \tag{5}$$

where K_r represents the values of the randomly chosen session key.
The logistic map is iterated by using the initial condition X, number of iterations N and system parameter r. The last value X_N is used for the encryption/decryption of plaintext/ciphertext in the following way:

$$C_i = (P_i + [X_N \cdot 256]) \, mod 256 \tag{6}$$

$$P_i = (C_i + 256 - [X_N \cdot 256]) \, mod 256 \tag{7}$$

where P_i and C_i are the decimal values corresponding to the block of the plaintext and ciphertext, respectively.
For the encryption/decryption of the next block of plaintext/ciphertext, X_N and C_{i-1} (the value of the previously ciphertext block) are taken as seed values for the initial condition (4) and the number (5), respectively. In this way, a feedback mechanism is used to make the cryptosystem more robust, encryption/decryption of the next block of plaintext/ciphertext depending on the history of encryption/decryption.

6. Performances of the Chaotic Cryptosystems

6.1. Sensitivity to a small change of parameter or initial condition

The chaotic cryptosystems that we have presented have the property of sensitivity to a small change of initial condition or parameter. To show this, we took a plain text and we changed every element of the Baptista cryptosystem key. We changed with a small value the set of elements of the cryptosystem's key, the initial condition x_0, the chaotic map parameter r, and the domain of the chaotic map X through the value x_{min}. We have considered as the plain message the word "text". The ciphertexts that are obtained in all the situations mentioned above are presented in table 1.

Table 1: The ciphertexts for Baptista method

	Plaintext/Ciphertext			
Key of the cryptosystem	t	e	x	t
Initial state	1173	2368	1185	801
$x_0^{'} = x_0 + 10^{-6}$	1192	482	4835	344
$r^{'} = r + 10^{-6}$	3441	1248	284	435
$x_{min}^{'} = x_{min} + 10^{-3}$	1736	2420	570	376

The initial state of the key elements is:

$$\begin{cases} x_0 = 0.34 \\ r = 3.996 \\ \eta = 0 \\ X = [x_{min}, x_{max}] = [0.2, 0.8] \end{cases} \tag{8}$$

If we look in the columns of the table 1, we can see distinct values that prove the behavior of the chaotic cryptosystem which is sensitive to any change in the key system although this change is very small $\left(10^{-6}\right)$. This property of the chaotic cryptosystem is similar with the confusion specific for the classic cryptosystems. We can observe also that the same letter "t" from the plain message (the first and the last letter) has as correspondent different ciphertexts in all the situations.

6.2. Diffusion

To show that chaos-based cryptosystem has the property of diffusion specific for classic cryptography we can use the cryptosystem that use external key. This cryptosystem will map the given plaintext into a random cipher-text, which means that no pattern appears in the ciphertext. The distribution of the ASCII values for a plaintext of approximate 1000 characters is presented in figure 4. In this plaintext most of the characters are lowercase, so the distribution is dense in the interval around 100 (figure 4).We have also presented

the ASCII value distribution of the corresponding ciphertext using a 128-bits secret key in figure 4. We observe that cipher-text distribution is almost uniform in the complete interval of ASCII values and hence the external key cryptosystem also maps plaintext to a random ciphertext.

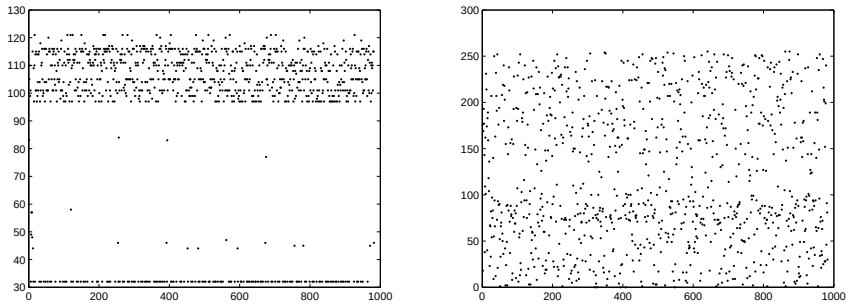

Figure 4: Distribution of the plain/crypto text for the external key method

6.3. Remarks about chaotic ciphers

Regarding dynamical degradation of digital chaos, for digital chaotic ciphers, some other problems should also be considered carefully in order to avoid possible weaknesses and promote the overall performance of designed ciphers. Such weaknesses include potential insecurity caused by the use of single chaotic system, slow encryption speed, and complex implementation because it means high implementation cost, etc. Although recently some problems have been noticed by researchers and some practical solutions have been proposed, there is not yet a comprehensive investigation on these problems and possible solutions. In [2], some typical problems are presented and also are suggested some practical solutions from both theoretical and experimental points of view. In the domain of digital chaos, there are two main considerations on the selection of chaotic systems used in digital cryptosystems:

- whether or not their dynamical properties are desired to ensure the security of designed ciphers?
- whether or not their implementations are simple enough for most application to save costs and reach fast encryption speed? In other words, the simpler the chaotic system is, the better the overall performance of the cipher will be.

The use of logistic map is clear because it is the most well-known chaotic system showing complex behaviors and one of the simplest chaotic systems but has some problems regarding periodic windows. The best chaotic map is the piece-wise linear chaotic map that has a good chaotic behavior for all the parameter possible values. The use of multiple chaotic

systems will be helpful to enhance security but it will make the system more complex. Nevertheless, in software implementations, you need a simplest chaotic system to reach fast encryption speed. Regarding this aspect, reasons of low encryption speed of most chaotic ciphers was investigated and one principle to promote encryption speed was given: the simpler the chaotic system is, the faster the cryptosystem will be.

7. Conclusions

The quantity of stored and processed data is permanently increasing, so the future research should be focused on finding new solutions not in order to add methods based on creating ad-hoc new ways of dealing with the problem, but to use the chaos-based methods in addition to the classic encryption ones. As we all know, the recent efforts of working in the block cryptology have been influenced by the differential and linear cryptanalysis, aspect that proves once again the importance of cryptanalysis in cryptology. That is, any new attack against chaotic methods will be a new impulse to work on improving these new information security resources, as digital chaotic systems can be used to create ciphers with satisfactory results. The chaotic ciphers suggested up to the present have been sorted out, analyzed and compared, and a few of the problems have been mentioned during the process of designing the codes. We believe that, if we would find solutions to eliminate these deficiencies, we could obtain systems able to provide good cryptographic properties. The application of dynamical chaotic systems for the development of new chaos-based algorithms is continuously evolving along with technology. Many of the methods proposed are in their initial state, due to the implementation technology. The communication systems that use chaos theory exceeded the stage of the laboratory simulations using Matlab or another designing tool and pass in the physical implementation step with component subsystems and certain applications. As technology develops, and the processing speed increases, hardware implementations become more and more adequate. A high throughput of one chaotic generator can be obtained using dedicated circuits (ASICs), field programmable logic arrays (FPGAs) or fast general purpose processors.

References

[1] Alvarez, G., Hernndez, L., Muoz, J., Montoya, F., Li, S., *Security analysis of communication system based on the synchronization of different order chaotic systems*, Physics Letters A, **345**, Issues 4-5 (2005), 245-250.

[2] Alvarez, G., Li, S., *Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems*, International Journal of Bifurcation and Chaos **16**, no. 8 (2006), 2129-2152.

[3] Baptista, M.S., *Cryptography with chaos*, Physics Letters A **240**, Issue 1-2 (1998), 50-54.

[4] Chen, J.Y., Wong, K.W., Cheng, L.M., Shuai, J.W., *A secure communication scheme based on the phase synchronization of chaotic systems*, Chaos **13** (2003), 508-514.

[5] Jakimoski, G., Kocarev, L., *Analysis of some recently proposed chaos-based encryption algorithms*, Physics Letters A **291**(6) (2001), 381-384.

[6] Kocarev, L., *Chaos-based cryptography: A brief overview*, IEEE Circuits and Systems Magazine **1** (2001), 6-21.

[7] Kocarev, L., Halle, K.S., Eckert, K., Chua, L.O., Parlitz, U., *Experimental demonstration of secure communications via chaotic synchronization*, Int. J. Bifurc. Chaos **2** (1992), 709-713.

[8] Lee, P.H., Pei, S.C., Chen, Y.Y., *Generating chaotic stream ciphers using chaotic systems*, Chinese J. Phys. **41** (2003), 559-581.

[9] Li, S., Mou, X., Cai, Y., *Pseudo-random bit generator based on couple chaotic systems and its application in stream-ciphers cryptography*, in Progress in Cryptology INDOCRYPT 2001, Springer-Verlag, Lecture Notes in Computer Science, vol. 2247, 316-329, 2001.

[10] Li, S., Chen, G., Wong, K.-W., Mou, X., Cai, Y., *Baptista-type Chaotic Cryptosystems: Problems and Countermeasures*, Phys. Lett. A **332**, No. 5-6 (2004), 368-375.

[11] Lu, H., Wang, S., Li, X., Tang, G., Kuang, J., Ye, W., Hu, G., *A new spatiotemporally chaotic cryptosystem and its security and performance analyses*, Chaos **14** (2004), 617-629.

[12] Masuda, N., Aihara, K., *Cryptosystems with discretized chaotic maps*, IEEE Trans. Circuits Syst. I **49** (2002), 28-40.

[13] Masuda, N., Jakimoski, G., Aihara, K., *Chaotic Block Ciphers: From Theory to Practical Algorithms*, IEEE Transactions on Circuits and Systems, **53**, No.6 (2006), 1341-1352.

[14] Memon, Q., *Synchronized chaos for network security*, Comp. Comm. **26** (2003), 498-505.

[15] Pecora, L.M., Carroll, T.L., *Synchronization in chaotic systems*, Physics Letters A, **64**, Issue 8 (1990), 821-824.

[16] Tang, G., Liao, X., Chen, Y., *A novel method for designing S-boxes based on chaotic maps*, Chaos Solitons Fractals **23** (2005), 413-419.

[17] Wong, K.-W., Man, K.-P., Li, S., Liao, X., *A more secure chaotic cryptographic scheme based on dynamic look-up table*, Circuits, Systems & Signal Processing **24** (2005), 571-584.

[18] Wong, K.-W., *A combined chaotic cryptographic and hashing scheme*, Physics Letters A **307**, Issues 5-6 (2002), 292-298.

[19] Wong, K.-W., "A fast chaotic cryptographic scheme with dynamic look-up table", Physics Letters A, Volume 298, Issue 4, pp. 238-242, Jun. 2002

[20] Pareek N.K., Patidor Vinod, Sud, K.K., "Discrete chaotic cryptography using external key", Elsevier Physic Letters A, Volume 309, Issue 1-2, pp 75-82, Mar. 2003