ON THE CHAOS-BASED CRYPTOGRAPHY USING CLASSICAL CRYPTOGRAPHIC ALGORITHMS

Ion Tutănescu, Emil Sofron

University of Piteşti, Romania

Abstract **- A growing attention has been given in the recent years to the chaos-based techniques for using them in the field of secure communication. In this paper we present a methodology for designing the chaotic-based cryptosystems. For the simulation of such a cryptosystem we used the Matsumoto-Chua-Kobayashi circuit.**

I. INTRODUCTION

There were developed several methods in order to improve the security level of the chaotic carrier communications. Basically, these methods use classical cryptographic algorithms in the structure of the chaotic systems.

In this domain there are several ways to approach this problem, existing already many "schools": the "british school" [3][4], the "german school" [5] and the "american school" [8]. In the papers presented until now there are proposed different methods to realise cryptographic systems.

A first direction to be followed is to use schemes based on digital filters. The second class of methods refers to the use of two chaotic signals: one for encrypter and decrypter synchronisation, the other one for the encryption itself.

New methods were proposed, combining the classic encryption with the synchronisation of chaotic systems. For enhancing the interception resistance of chaotic carrier communications, there were proposed methods that use classical cryptography blocks in the same structure with the chaotic systems.

II. CHAOS-BASED CRYPTOGRAPHY USING DIGITAL FILTERS

There are presented in [3] and [4] digital filters-based chaotic systems. It was demonstrated in [1] and [2] that the digital filters can be used in the construction of some chaotic systems. It was shown in [3] that digital filters with finite precision have a quasi-chaotic behaviour, that gives them following properties, named Quasi Chaos-properties (*QC*-properties):

- the filter response (without having any input) has a noise-like spectrum for all possible selections of initial conditions; the noise-like signal is defined as a filtered version of the white gaussian noise.
- the filter response to an arbitrary input has a noise-like spectrum for all possible selections of initial conditions, too.
- the filter response to almost all (90-95%) arbitrary inputs is uncorrelated with input for almost all possible selections of initial conditions.
- the filter response to the same inputs are uncorrelated for almost all possible selections of initial conditions.
- two filters' states will be different for almost all possible selections of inputs in two identical filters, having different but close initial states.

The digital filter-based encrypter must have QC-properties in order to have a quasi-chaotic behaviour and therefore to be of value in secure communications applications [3]. The encrypter having QC-properties can be used for securing the communication.

The encrypter and the decrypter obey the following defining equations:

a) Encrypter

$x(n) = h_1(n) * u(n) + h_2(n) * F(x(n), x(n - 1), \ldots, x(n - M));$

$e(n) = d(n) * x(n);$

b) Decrypter

$x(n) = \bar{d}(n) * e(n);$

$x(n) = \bar{h}_1(n) * u(n) + \bar{h}_2(n) * F(x(n), x(n - 1), \ldots, x(n - M));$

where:

- $u(n)$ - the input sequence (plaintext signal);
- $x(n)$ - an internal signal;
- $e(n)$ - the encrypted signal to be transmitted to the receiver;
- $y(n)$ - the output sequence (decrypted signal);
- $h_1(n), h_2(n), \ldots$ - IIR *(Infinite Impulse Response)* or FIR (*Finite Impulse Respo*nse).
- $F(.)$ - a general non-linear map suited to hardware implementation.
- $+$ *and* $*$ - the addition and convolution operators.

The encrypter must respect the QC-properties and the decrypter must realise the inverse function of the encrypter.

Such a cryptographic system whose operation is based on equations

$$e(n) = u(n) + \{e(n - 1) + f(e(n - 2))\};$$
$$y(n) = e(n) - \{e(n - 1) + f(e(n - 2))\}.$$

is presented in Fig. 1:

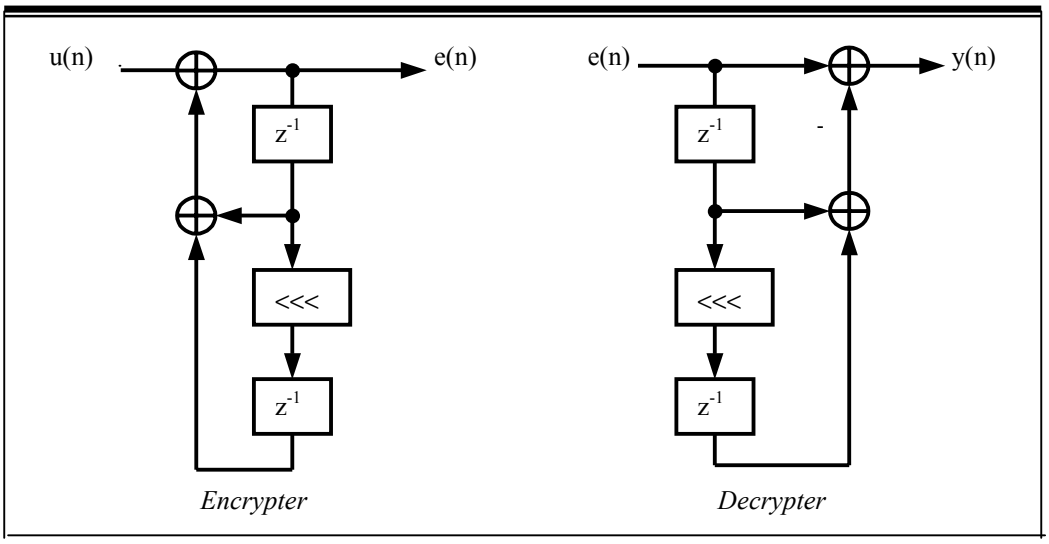

Fig. 1. Digital filter-based cryptographic system.

where <<< is a left circular rotation function.

The approach proposed in [5] uses:

- digital filters for the chaotic systems construction,
- binary shift registers, shift ciphers and auto-key ciphers for encryption and decryption.

A chaotic cryptosystem using FIR digital filters and a Least Mean Square (LMS) adaptation algorithm and also the obtained simulation results were presented in [6].

III. CHAOS-BASED CRYPTOGRAPHY USING CLASSICAL CRYPTOGRAPHIC ALGORITHMS

A different approach [7] [8] uses two chaotic signals: one of them is used for the chaotic encrypter and decrypter synchronisation and the other signal is used for informational signal encryption using a encryption scheme, by example with shift ciphers. The general block diagram of the chaos-based cryptosystem is represented in Fig. 2.

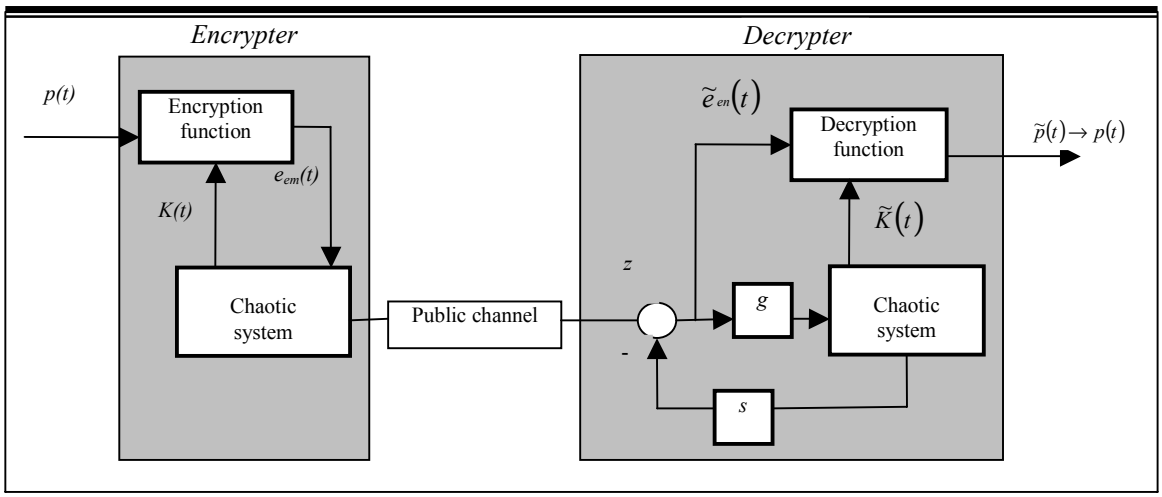

Fig. 2. Block diagram of the chaos-based cryptosystem.

The *encrypter* consists of a chaotic system and an encryption function *e(t)*. The cryptographic key *k(t)* is one of the state variables of the chaotic system. The transmitted signal *s(t)* is another state variable of the chaotic system. It is sent through a public channel to the decrypter and used to synchronise the decrypter.

The *decrypter* consists of a chaotic system and a decryption function *d()*. It should be noted that both the encrypted signal *y(t)* and the key signal *k(t)* are not sent to the decrypter. It is different from traditional discrete cryptosystems where both the encrypted signal and the key should be transmitted to the decrypter.

The communication channel's noise *n(t)* is added to *s(t),* so the decrypter receives the sum signal *s(t) + n(t).*

Only when the decrypter and the encrypter are synchronised, the decrypter can find the encrypted signal and the key signal. Then, the decryption function *d()* is used to decrypt the encrypted signal.

IV. THE DESIGN OF A CHAOS-BASED CRYPTOSYSTEM USING CLASSICAL CRYPTOGRAPHIC ALGORITHMS

The proposed cryptosystem block diagram to design is that shown in Fig. 2. The central idea is realising the decrypter as a *non-linear observer* for the state of the encrypter. An observer is a dynamic system designed to be driven by the output of another dynamic system. The observer has the property that its state converges to the state of the other system.

According to this approach, the cryptosystem design consists of *four* stages:

a) The first of them proposes the establishment of chaotic system *state equations*:

$$\dot{x} = Ax + bf(x) + c, \qquad (1)$$

where:

$x \in R^{nx1}$, $A \in R^{n\,x\,n}$, $b \in R^{n\,x\,1}$, $c \in R^{n\,x\,1}$ and $f: R^n \to R$.

b) In the second stage the *encryption function* for a given plaintext signal *p(t)* is set:

$$e_{en}(t) = e_{en}(p(t), K(t)), \qquad (2)$$

where $e_{en}(.)$ is the encryption function that uses the key signal *K(t)*.

Using symmetric algorithms, the plaintext message *p(t)* is obtained from the ciphertext $e_{en}(t)$ on the basis of relation:

$$p(t) = d(e_{en}(t), K(t)), \qquad (3)$$

where *d(.)* is the decryption function.

c) In the third stage the *encryption system* is considered as a dynamic system described by the equations:

$$\dot{x} = Ax + bf(x) + c + b\,e_{en}(t). \qquad (4)$$

The retrieval of the original message (plaintext) assumes the key generation at the receiver and the synchronisation between the encrypter and the decrypter.

d) The fourth stage defines the *decryption system* for the given encryption system (4) as being the dynamic system described by:

$$\dot{y} = Ay + bf(y) + c + g(z - s(y)), \qquad (5)$$

where $g: R \to R^n$ is a non-linear function, *z(t)* is a scalar signal transmitted through the public (unprotected) channel and *s(y)* is a scalar output of the chaotic system.

The decryption system (5) must be designed so that *y* converges to state *x* when $t \to \infty$, i.e. $e(t)=[y(t) - x(t)] \to 0$ as $t \to \infty$ (where *e* is the synchronisation error).

If $e(t) \to 0$ when $t \to \infty$ for any initial condition $(y(0), x(0))$, we can say that the decryption system (5) is a global observer of the encryption system (4).

For illustrating the proposed approach the chaos-based cryptosystem with *Matsumoto - Chua - Kobayashi* circuit was used. The above mentioned circuit has the following state equations:

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \\ \dot{x}_4 \end{bmatrix} = \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0{,}7 & 0 & 0 \\ 0 & 0 & 0 & +10 \\ 0 & 0 & 1{,}5 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} + \begin{bmatrix} -1 \\ 0 \\ 10 \\ 0 \end{bmatrix} g(x_1, x_3), \quad (6)$$

where $\dot{x}_i = \frac{dx_i}{dt}$ and *g(.)* is a linear function on sections, given by:

$$g(x_1, x_3) = \begin{cases} -0{,}2 + 3(x_1 - x_3 + 1), & for\ \ x_1 - x_3 < -1; \\ -0{,}2(x_1 - x_3), & for\ \ -1 \le x_1 - x_3 \le 1; \\ -0{,}2 + 3(x_1 - x_3 - 1), & for\ x_1 - x_3 > 1. \end{cases} \quad (7)$$

For the plaintext encryption is used an n-shift cipher:

$$e_{en}(t) = f_1(\ldots f_1(f_1(p(t), K(t)), K(t)), \ldots, K(t)), \qquad (8)$$

where:

$$f_1(x, K) = \begin{cases} (x + K) + 2h, & for\ -2h \le (x + K) \le -h; \\ (x + K), & for\ -h < (x + K) < -h; \\ (x + K) - 2h, & for\ \ h \le (x + K) \le 2h. \end{cases} \quad (9)$$

with $h = 5$ şi $n = 5$.

The transmitted signal in the public channel is:

$$z(t) = g(x_1, x_3) + \sum_{i=1}^{4} k_i x_i + e_{en}(t). \qquad (10)$$

V. THE SIMULATION RESULTS

The input plaintext signal used for simulation were: a) $p(t) = sin\ t$; b) $p(t)$ - binary signal (randomly generated). The encryption key $K(t) = x_4(t)$ was chosen.

For the simulation we realised a program in Matlab. In Fig. 3a and in Fig. 3b we present the obtained results for the sinusoidal and binary input signals, respectively.

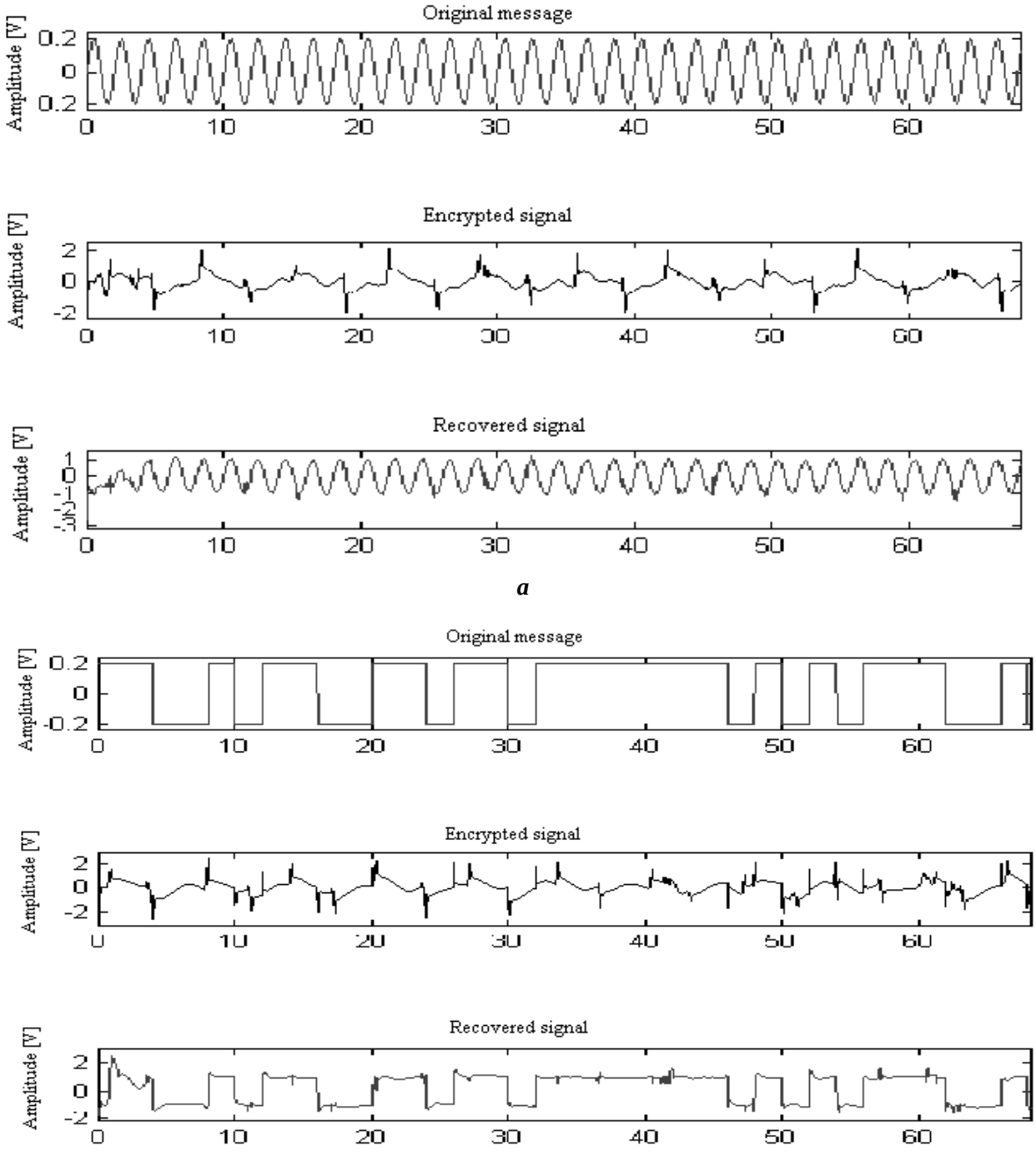

Fig. 3. Time waveforms for the sinusoidal input signal (a) and binary input signal (b): original signal - *up*, encrypted signal - *middle* and recovered signal - *down*.

VI. CONCLUSION

Basically, to increase the interception resistance of the chaotic carrier communications three classes of methods are used:

a. the use of digital filters having QC-properties together with non-linear mapping functions,

b. the use of digital filters having a chaotic behaviour together with binary shift registers, shift cipher and auto-key ciphers,

c. the use of chaotic systems involving two chaotic signals: first for the chaotic encrypter and decrypter synchronisation and the other for informational signal encryption using a classical encryption algorithm (by example with shift ciphers).

In order to enhance the interception resistance of chaotic carrier communications, there were realised other methods which use classical cryptographic blocks in the same structure with the chaotic systems.

The proposed cryptosystem in this paper offers a good security level. It is known that the more complex is the transmitted signal, the higher is the security of the communication system. The designed cryptosystem delivers in the public channel a very complex signal: transmitted signal z consists of three summed signals - the chaotic signal $f(x)$, the linear combination of all chaotic state variables kx and the encrypted signal $e_{en}(t)$.

A good advantage of the described methodology is that the cryptosystem design is very flexible. The proposed cryptosystem can include also other chaotic system (Chua, Rossler, etc.).

REFERENCES:

[1] Chua L.O., Lin T. - "Chaos in digital filters", IEEE Transactions on Circuits and Systems, Vol. 35, June 1998, pag. 648-658;

[2] Chua L.O., Lin T. - "Chaos and fractals from third-order digital filters", Int. J. Circuit Theory Applications, Vol. 18, May-June 1990, pag. 241-255;

[3] Frey D.R. - "Chaotic Digital Encoding: An Approach to Secure Communication", IEEE Transactions on Circuits and Systems - II: Analog and Digital Signal Processing, Vol. 40, No. 10, October 1993, pag. 660-666;

[4] Frey D.R. - "On Adaptive Chaotic Encoding", IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications, Vol. 45, No. 11, November 1998, pag. 1200-1204;

[5] Götz M., Kelber K., Schwarz W. - "Discrete-Time Chaotic Encryption Systems - Parts I, II and III, IEEE Transactions on Circuits and Systems - I: Fundamental Theory and Applications, Vol. 44, No. 10, October 1997, pag. 963-970/ Vol. 45, No. 2, February 1998/ Vol. 45, No. 9, September 1998, pag. 983-988;

[6] Tutănescu I., Călugăreanu M., Irimia C. – "A chaotic digital cryptosystem", 3rd International Conference on Renewable Sources and Enviromental Electro-Technologies RSEE'2000, Oradea, 25-27 May 2000, ISSN 1454-9239;

[7] Tutănescu I., Irimia C., Şerbănescu A. - "Design and simulation of a chaotic based cryptosystem", International Conference "Communications 2000", Bucharest, 7-9 December 2000;

[8] Yang T., Wu C. W., Chua L.O.- "Cryptography Based on Chaotic Systems", IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications, Vol. 44, No. 5, May 1997, pag. 469-472;

[9] Grassi G., Mascolo S. - "A System Theory Approach for Designing Cryptosystems Based on Hyper-chaos", IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications, Vol. 46, No. 9, September 1999, pag. 1135-1138;

[10] Carroll T. L., Pecora L. M. - "Synchronising Chaotic Circuits", IEEE Transactions on Circuits and Systems - I: Fundamental Theory and Applications, Vol. 38, No. 4, April 1995, pp. 453-456;

[11] Corron N. J., Hahs D. W. - "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.