Towards an Encryption Scheme Based on Hybrid Systems

Juan Gonzalo Barajas Ramírez, Ricardo Femat and Ilse Cervantes

***Abstract*— On this contribution, a hybrid time system that evolves switching between two continuous-time vector fields, one stable and the other unstable, is used to construct a secure communication scheme. The proposed cypher encrypts information on the trajectories of a hybrid time system with a switching rule chosen such that the system presents complex behavior. A motivation for this study is to investigate the effects of the switched nature of the hybrid-time system on the implementation, realization and performance of an encryption system. One significant characteristic of hybrid-time systems is their simplicity of construction, which may represent an advantage in practical implementations. As an initial investigation, a hybrid time system is used to construct a symmetric block cypher, where the encryption-decryption process is defined in terms of a stroboscopic map of the system trajectories. In this way, the information signal is transformed into a signal that can be transmitted over a public channel and requires from an authorized receiver the use of the transmitter's hybrid time system trajectories to recover the original message. In order to illustrate the proposed encryption scheme, numerical simulations have been performed.**

I. Introduction

Over the last couple of decades researchers have actively investigated many possible applications of nonlinear dynamics to communications and information transmission. A central issue in these investigations has been the study of chaos-based encryption schemes (see [3], [5], [7] and some references therein).

Cryptographical systems are characterized by two basic properties: confusion and diffusion. A cypher has the property of confusion if its output has basically the same probability distribution function for any input. Moreover, the cypher also has the diffusion property which means that a small deviation in the input causes a large change on the cypher's output [1], [4], [6]. From their part, complex chaotic dynamics are characterized by ergodicity and sensitivity to initial conditions. The tight relationship between the properties of conventional cryptosystems and complex dynamics has resulted on the proposal of several chaos-based encryption schemes designed to compete with conventional secure communication systems [3], [5].

The main difference between conventional and dynamical system based encryption (DSBE) is as follows: Conventional cryptography operates on discrete valued elements that evolve on discrete-time, which means that they can be designed using tools from number theory, relaying on computational complexity to achieve their security characteristics. On the other hand, encryption schemes based on dynamical systems use sections or the entire trajectory of the system to encrypt a message, these are continuous valued elements that evolve on continuous or discrete time, depending on the nature of the system used for encryption. In this case, the cypher can not be designed or analyzed using the same tools as for conventional encryption systems. Ultimately, the security characteristics of a dynamical system based cypher can be analyzed statistically, in terms of how well the information gets hidden by the encryption system.

For the most part, the research on DSBE has been carried out considering either continuous or discrete time systems, while hybrid systems have not been explicitly considered. In terms of their applicability as cyphers, hybrid systems have significant potential due to the fact that their dynamical evolution depends on logical conditions given in terms of both states and time constrains, such logical conditions result on a wide range of possible encryption keys, which in turn may provide a hybrid time DSBE scheme with good security characteristics.

In order to analyze the effects of using a hybrid time system as part of an encryption scheme, we consider a symmetric public channel secret key structure, as depicted on Figure 1, where m is the plaintext message; c is the cyphertext to be transmitted over the public channel; and k is the encryption key, here the parameters of the hybrid-time system. The encryption and decryption maps $e(\cdot)$ and $d(\cdot)$ are defined in terms of the stroboscopic values of the hybrid systems and are chosen such that $m = d(x_R, e(x_T, k))$. The initial results indicate that hybrid time systems are a viable alternative for the design of a DSBE with good security characteristics.

The remainder of the paper is organized as follows: In Section 2, the hybrid-time system used in the encryption process is described. In Section 3, the proposed symmetric cypher and the encryption-decryptions processes are described in detail. The encryption characteristics of the hybrid time cypher are statistically analyzed in Section 4 and numerical simulations are presented to illustrate its effectiveness. Finally, on Section 5, some comments and conclusions are presented.

II. Hybrid time System

The DSBE scheme proposed in this paper is constructed using a hybrid time system given by [2]:

$$\dot{\xi}(t) = A_i \xi(t) + B(t) \qquad (1)$$

where $\xi(t) = [\xi_1(t), \xi_2(t)]^\top \in \mathbf{R}^2$ are the state variables of the system; $B(t) = B_1 + B_2(t)$ represents the inputs to the system, defined as a constant input $B_1 =$

All are with Laboratorio de Biodinámica y Sistemas Alineales, DMAp-IPICyT, Apdo Postal 3-90, Tangamanga, CP 78231, San Luis Potosí, S.L.P., México; jgbarajas@ipicyt.edu.mx

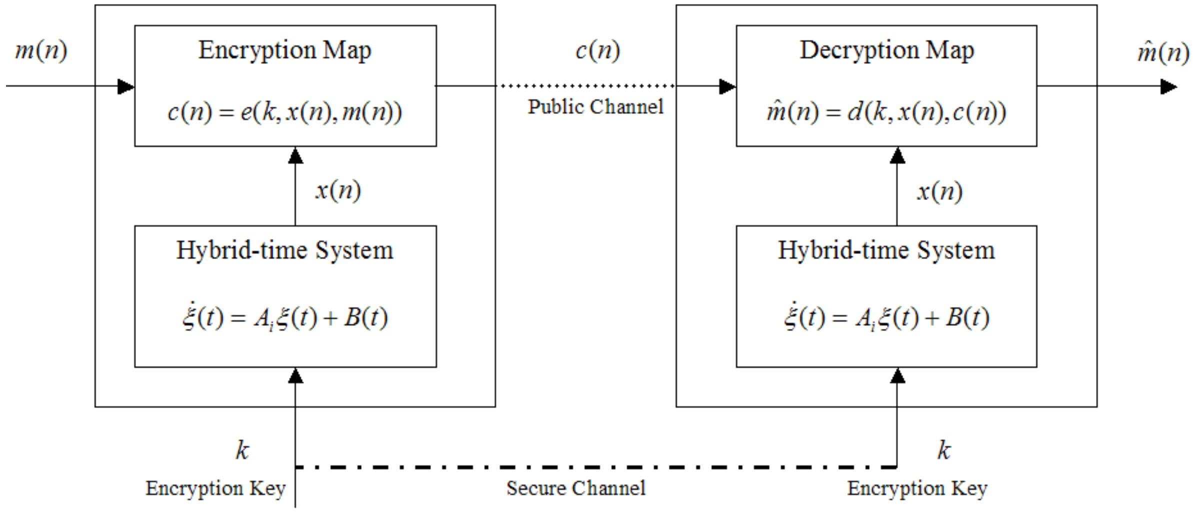

Fig. 1. Structure of the Symmetric Public Channel Secret Key encryption scheme

$[\alpha_1, \alpha_2]^\top \in \mathbf{R}^2$, and a periodic excitation $B_2(t) = [\beta_1 \sin(\omega t), \beta_2 \sin(\omega t)]^\top \in \mathbf{R}^2$.

The values of the matrix $A_i \in \mathbf{R}^{2\times 2}$ for $i = 0, 1$ are determined by the following rule:

$$A_i = \begin{cases} A_0, & \text{if } \ D = 0 \\ A_1, & \text{if } \ D = 1 \end{cases} \tag{2}$$

The matrices A_0 and A_1 are given in their controller canonical form, and their entries are such that: A_0 describes a stable system; while A_1 describes an unstable one. In this way, the dynamics of the system when $D = 0$ correspond to a dissipation regime, and when $D = 1$, the dynamics are in an accumulation stage.

The switching condition is established according to the following criteria:

$$D = \begin{cases} 0, & \text{if } \ \xi_1(t) \geq \xi_{ref} \\ 1, & \text{if } \ t = nT_s \end{cases} \tag{3}$$

for $n = 0, 1, 2, ...$ where $T_s > 0 \in \mathbf{R}$ is a constant switching period.

One way to visualize the dynamics of (1)-(3) is using a stroboscopic map at each switching period T_s. The resulting discrete-time variables ($x(n) = [x_1(n), x_2(n)]$) are use to encrypt the information signal according to the algorithm presented in the following Section.

III. Description of the Proposed Block Cypher

Using the hybrid time system described in the previous Section the symmetric cypher presented in Figure 1 is realize by the following encryption-decryption algorithm:

Step 1: The hybrid time system in (1)-(3) is integrated for a given parameter set and initial conditions (ρ, $\xi(0)$). Then, a stroboscopic map of the resulting trajectory is taken every switching period. That is, the trajectory is sampled such that

$$x(n) = \xi(nT_s)$$

for $n = 0, 1, 2, ..., N$.

Step 2: The sampled states of the hybrid time $x(n)$ are normalized and offset, such that

$$x(n) \to \hat{x}(n) = \frac{x(n) - x_{min}}{x_{max} - x_{min}} + 1 \in [1, 2]$$

where x_{min} and x_{max} are the minimum and maximum values of $x(n)$. Then, the same process is applied to the information signal $m(n)$, such that

$$m(n) \to \hat{m}(n) \in [1, 2]$$

In this way every value considered is positive and different from zero.

Step 3: The current value of the information signal is encrypted in terms of the stroboscopic map of the hybrid time system and the previously encrypted values of the information signal, according to the following formula:

$$c(n) = \frac{\hat{x}_2(n)}{T_s} + \frac{\hat{m}(n)\hat{x}_1(n-1)T_s}{c(n-1)} \tag{4}$$

where $c(n)$ is the current point of the information signal being encrypted and $c(n-1)$ is the previously encrypted point. For consistency, the initial value of the encrypted signal is set to one ($c(0) = 1$).

Step 4: The inverse of the encryption map (4) is given by

$$\hat{m}(n) = \frac{(c(n) - \frac{\hat{x}_2(n)}{T_s})c(n-1)}{\hat{x}_1(n-1)T_s} \tag{5}$$

Since, the current and previous values of $\hat{x}(n)$ and $c(n)$ are available, the information signal can be decrypted from the received signal by an authorized receiver having the correct encryption key.

Step 5: The original information signal $m(n)$ is obtained, applying the following formula

$$m(n) = (\hat{m}(n) - 1)m_r + m_{min} \tag{6}$$

where $m_r = m_{max} - m_{min}$ with m_{min} and m_{max} the minimum and maximum values of the information signal, respectively.

The encryption key is generated by grouping together the parameters of the hybrid time systems ($\rho = \{A_i, B(t), \xi_{ref}\}$), the chosen initial condition (ξ_o), the stroboscopic period (T_s) and the minimum and maximum values of the information signal (m_{min} and m_{max}). These values are made available to an authorized receiver through a secure channel, as shown in Figure 1.

IV. Initial Cryptanalysis

The symmetric block cypher described above was numerically realized to encrypt a periodic information signal

$$m(n) = \sin(2\pi n), \qquad n = 1, ..., 1024 \tag{7}$$

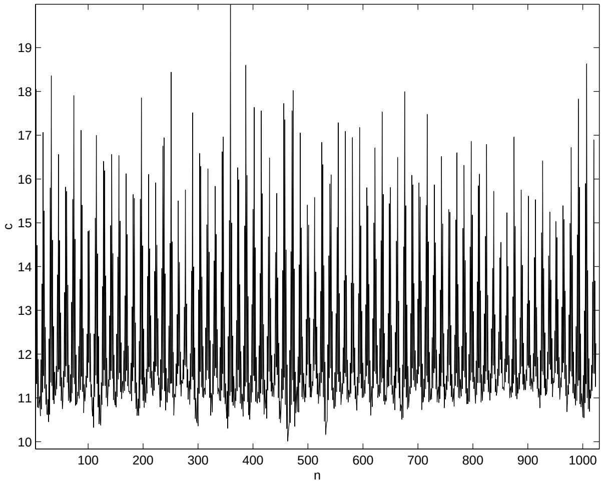

Fig. 2. Encrypted Signal $c(n)$ of the periodic information signal $m(n)$

To this end, the hybrid time system (1)-(3) was simulated for the parameter set: $\rho = \{A_0 = [0, 1; -3, -2]$; $A_1 = [0, 1; -3, 2]$; $\alpha_1 = 50$; $\alpha_2 = 30$; $\beta_1 = 45$; $\beta_2 = 27$; $\omega = 1.8$; $\xi_{ref} = 50\}$, and the initial condition $\xi_0 = [1, -3]$, with a sampling period of $T_s = 0.1$. From (7), one has that $m_{min} = -1$ and $m_{max} = 1$. With the above parameter set as encryption key the information signal (7) was converted into the encrypted signal $c(n)$ shown in Figure 2 by way of the encryption map (5). Using the decryption map (6) with the appropriated key parameters, the information can be recovered, as shown in Figure 3.

An initial test of the security provided by the proposed block cypher is to consider the case of an unauthorized receiver that will like to recover the information signal and somehow is able to obtain the secret encryption key except for the exact value of one parameter, lets say the reference level ξ_{ref}, the question is: Who much of the information signal can be obtain from the encrypted signal under these conditions? To investigate the above situation, the encrypted signal was decrypted following the algorithm presented in the previous Section for an error of 0.1% on the parameter ξ_{ref}, the message recovered in these conditions is shown in Figure 4, which is very different to the original message.

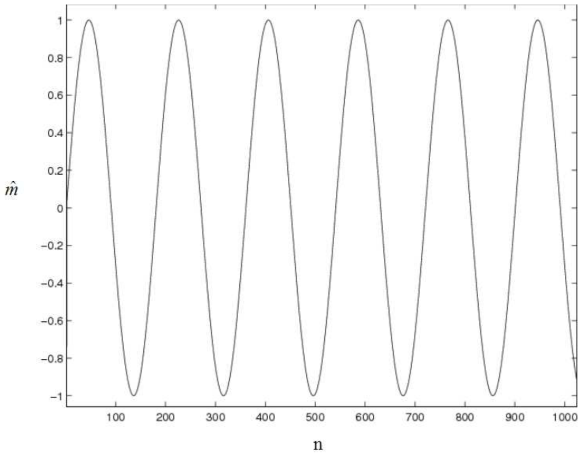

Fig. 3. Recovered information signal $\hat{m}(n)$ with the correct encryption key

An other way to test the security of the proposed DSBE scheme is estimate who well the information gets hidden in the encrypted signal. One way to evaluate this aspect of the cypher performance is to compare the Fourier spectrums of the information and the resulting encrypted signal. In Figure 5 the frequency spectrums of the information signal (7) and its corresponding encrypted signal are shown. It can be seen that the frequency information of the message is well hidden by the encryption scheme. These results indicate that the proposed DSBE has good diffusion characteristics and strong encryption keys.

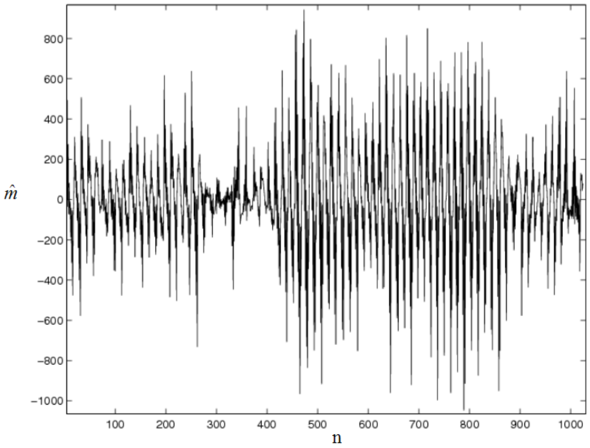

Fig. 4. Recovered information signal $m(n)$ with an encryption key that has a 0.1% error on the parameter ξ_{ref}

Next, we investigate the dependence of the encrypted signal ($c(n)$) on the message signal ($m(n)$). To this end, the proposed DSBE scheme is use to encrypt different periodic and uniformly distributed random signals. Then, measuring the correlation between the resulting encrypted signals the results shown in Figure 6 are obtained. These results indicate

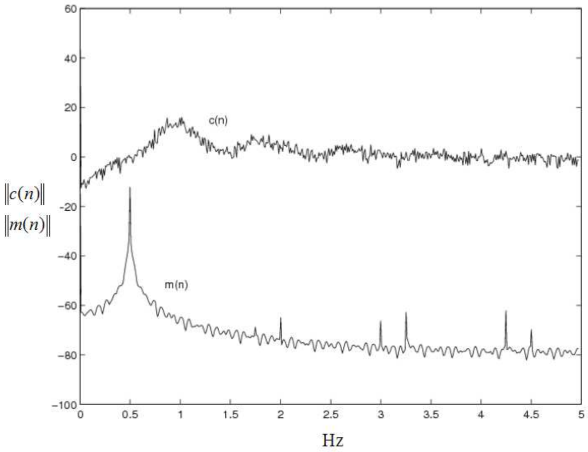

Fig. 5. Frequency spectrum for periodic message $m(n)$ and the corresponding encrypted signal $c(n)$

that the proposed DSBE has good confusion properties, since the output of the cypher is not message dependent.

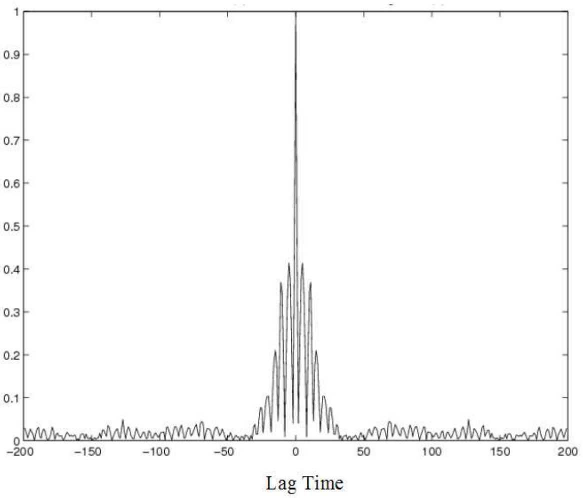

Fig. 6. Correlation between $c(n)$ for different information signal

V. Comments and Conclusion

On this contribution a symmetric block cypher based on hybrid time systems was proposed. The preliminary results show that a encryption scheme based on a hybrid time system has good diffusion and confusion characteristics. However, further analysis of the statistical properties of the key space and its resistance to attacks are needed.

The proposed DSBE scheme uses the simplest structure and most conventional approaches for analysis, as a result, the applicability maybe limited. Alternative encryption structures need to be considered, perhaps a stream cypher structure may prove more general. However, a stream cypher will suffer from the weaknesses common to most dynamical system encryption, their susceptibility to robust and generalized synchronization attacks. Yet, due to the hybrid nature of the proposed encryption system, the construction of a system capable of recovering the information by an unauthorized receiver will become a considerably more complicated problem than for a continuous or discrete time system. Estimating the effects on the security of an alternative encryption structure, and proposing improved versions of the scheme above, are contemplated as future work to the results presented in this contribution.

References

[1] Alvarez, G., Li, S. “Some basic cryptographic requirements for chaos-based cryptosystems”, Int. J. Bifurcation and Chaos, 16(8), 2124-2151, 2006

[2] Cervantes, I., Femat, R., Leyva Ramos, J. “Study of a class of hybrid-time systems”, Chaos, Fractals and Solitons, 32, 1081-1095, 2007

[3] Dachselt, F., Schwarz, W. “Chaos and cryptography”, Trans. Circ. Sys. I, 48, 1498-1509, 2001

[4] Kelber, K., Schwarz, W. “General Design Rules for Chaos-bases Encryption Systems”, 2005 NOLTA, Bruges, Belgium, 465-468, 2005

[5] Kocarev, L. “Chaos-based cryptography: A brief overview”, IEEE Cir Syst Mag., 1(3), 7-21, 2001

[6] Li, C., Li, S., Alvarez, G., Chen, G., Lo, K.T., “Cryptanalisis of two chaotic encryption schemes based on circular bit shift and XOR operations”, Phys Lett A, *in press*, 2007

[7] Mao, Y. B., Chen, G. “Chaos based image encryption”, in *Handbook of Computational Geometry for Pattern Recognition, Computer Vision, Neuralcomputing and Robotics*, ed. E. Bayro, Springer-Verlag, New York, pp 231-265, 2005