ISCAS 2000 - IEEE International Symposium on Circuits and Systems, May 28-31, 2000, Geneva, Switzerland

DRIVING CRYPTOSYSTEMS WITH HYPERCHAOTIC SIGNALS: AN APPROACH INVOLVING LINEAR OBSERVERS

Giuseppe Grassi (*) and Saverio Mascolo (**)

(*) Dipartimento di Ingegneria dell'Innovazione
Università di Lecce, 73100 Lecce, Italy
giuseppe.grassi@unile.it

(**) Dipartimento di Elettrotecnica ed Elettronica
Politecnico di Bari, 70125 Bari, Italy
mascolo@poliba.it

ABSTRACT

In this paper a method for designing cryptosystems driven by hyperchaotic signals is developed. The idea is to transmit a proper hyperchaotic signal, so that the receiver behaves as a linear observer for the state of the transmitter. The proposed tool proves to be: (i) rigorous, since some propositions are given for obtaining the plaintext at the receiver in a rigorous way; (ii) flexible, since a wide class of cryptosystems is designed by exploiting different hyperchaotic transmitting circuits; (iii) efficient, since the hyperchaotic carrier masks the encrypted signal, which in turn hides the message signal. The combination of hyperchaos, cryptography and complex transmitted signal makes a contribution to the development of communication systems with higher security.

1. INTRODUCTION

Different techniques have been recently proposed in order to hide the contents of a message by exploiting chaotic circuits. In order to enhance the level of security, the adoption of hyperchaotic systems is more advantageous than the use of simple chaotic ones [1]-[5].

The aim of this paper is to develop a general approach to cryptography based on hyperchaotic systems. The idea is to transmit a proper hyperchaotic signal, so that the receiver behaves as a linear observer for the state of the transmitter. The proposed approach presents the following advantages: (i) it assures that the plaintext is retrieved in a rigorous way; (ii) it enables different hyperchaotic circuits to be used; (iii) it is characterized by a high level of security, since the key (required for the decryption) is not transmitted over the channel.

The paper is organized as follows. The theoretical framework is reported in Section 2, whereas in Section 3 an example of hyperchaos-based cryptosystem is illustrated. Finally, in Section 4 the advantages of the proposed technique are discussed in detail.

2. THEORICAL FRAMEWORK

The proposed framework consists of four parts.

Part 1: The hyperchaotic system is described by the following state equations:

$$\dot{\boldsymbol{x}} = \boldsymbol{A}\boldsymbol{x} + \boldsymbol{b}\, f(\boldsymbol{x}) + \boldsymbol{c} \qquad (1)$$

where $\boldsymbol{x} \in \Re^{n\times 1}$, $\boldsymbol{A} \in \Re^{n\times n}$, $\boldsymbol{b} \in \Re^{n\times 1}$, $\boldsymbol{c} \in \Re^{n\times 1}$ and $f : \Re^n \to \Re$.

Part 2: Given a plaintext signal $p(t)$, the ciphertext is [1]:

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

where $e_{en}(\cdot)$ is a generic encryption function that makes use of a key $K(t)$. By adopting symmetric algorithms (i.e., by using the same key for encryption and decryption), the plaintext is obtained from the ciphertext $e_{en}(t)$ as follows:

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

where $d(\cdot)$ is the decryption function [1]. Since in chaotic cryptosystems the idea is to exploit (1) for generating the key signal $K(t)$, it is assumed that:

$$K(t) = K(\boldsymbol{x}(t)) \qquad (4)$$

0-7803-5482-6/99/$10.00 ©2000 IEEE

where K can be any generic function, i.e., $K:\Re^n \to \Re$.

Part 3: Given the chaotic system (1), the key (4) and the ciphertext (2), the encrypter (transmitter) is a dynamic system described by the equations:

$$\dot{\boldsymbol{x}} = \boldsymbol{A}\boldsymbol{x} + \boldsymbol{b}f(\boldsymbol{x}) + \boldsymbol{c} + \boldsymbol{b}\,e_{en}(t) \qquad (5)$$

In order to retrieve the plaintext, it is necessary to generate the key at the receiver. Herein, this objective is achieved by designing the receiver as a linear observer for the state of the transmitter. It should be pointed out that an observer is a dynamic system designed to be driven by the output of another dynamic system (plant) and having the property that the state of the observer converges to the state of the plant [6].

Part 4: Given the encrypter (5), the decrypter (receiver) is the *linear* dynamic system:

$$\dot{\hat{\boldsymbol{x}}} = \boldsymbol{A}\hat{\boldsymbol{x}} + \boldsymbol{c} + \boldsymbol{g}(z - s(\hat{\boldsymbol{x}})) \qquad (6)$$

where $\boldsymbol{g}:\Re^n \to \Re^n$ is suitably chosen nonlinear function, $z(t)$ is the scalar signal that is transmitted through a public channel, whereas $s(\hat{\boldsymbol{x}})$ is a scalar output of system (6). By taking into account the previous considerations, (6) has to be designed so $\hat{\boldsymbol{x}}(t) \to \boldsymbol{x}(t)$ for large t, that is, $\boldsymbol{e}(t) = (\hat{\boldsymbol{x}}(t) - \boldsymbol{x}(t)) \to \boldsymbol{0}$ for large t, where $\boldsymbol{e}$ represents the error between system (6) and (5). If $\hat{\boldsymbol{x}}(t) \to \boldsymbol{x}(t)$ for any initial condition $\hat{\boldsymbol{x}}(0), \boldsymbol{x}(0)$, system (6) is said to be a global observer of system (5) [3].
Now two propositions are given, which enable the plaintext to be retrieved in a rigorous way if a structural property of system (1) holds.

Proposition 1: If the $n \times n$ matrix

$$\left[\boldsymbol{b} \quad \boldsymbol{A}\boldsymbol{b} \quad \boldsymbol{A}^2\boldsymbol{b} \quad \ldots \quad \boldsymbol{A}^{n-1}\boldsymbol{b}\right] \qquad (7)$$

is full rank, then the decrypter (6) becomes a global observer of the encrypter (5) by taking

$$\boldsymbol{g}(z - s(\hat{\boldsymbol{x}})) = \boldsymbol{b} \cdot (z - s(\hat{\boldsymbol{x}})) \qquad (8)$$

$$z(t) = f(\boldsymbol{x}) + \boldsymbol{k}\boldsymbol{x} + e_{en}(t) \qquad (9)$$

$$s(\hat{\boldsymbol{x}}) = \boldsymbol{k}\hat{\boldsymbol{x}} \qquad (10)$$

where $\boldsymbol{k} = [k_1, k_2, \ldots k_n] \in \Re^{1\times n}$ must be chosen so that the eigenvalues of $(\boldsymbol{A} - \boldsymbol{b}\boldsymbol{k})$ lie in the open left half plane.

Proof: By making use of (8)-(10), the error system between (6) and (5) can be written as:

$$\begin{aligned}\dot{\boldsymbol{e}} &= \boldsymbol{A}\hat{\boldsymbol{x}} + \boldsymbol{c} + \boldsymbol{g}(z - s(\hat{\boldsymbol{x}})) \\ &\quad - (\boldsymbol{A}\boldsymbol{x} + \boldsymbol{b}f(\boldsymbol{x}) + \boldsymbol{c} + \boldsymbol{b}\,e_{en}(t)) \\ &= \boldsymbol{A}\boldsymbol{e} + \boldsymbol{b}(f(\boldsymbol{x}) + \boldsymbol{k}\boldsymbol{x} + e_{en}(t) - \boldsymbol{k}\hat{\boldsymbol{x}}) \\ &\quad - \boldsymbol{b}f(\boldsymbol{x}) - \boldsymbol{b}\,e_{en}(t)\end{aligned}$$

that is: $$\dot{\boldsymbol{e}} = \boldsymbol{A}\boldsymbol{e} - \boldsymbol{b}\boldsymbol{k}\boldsymbol{e} = \boldsymbol{A}\boldsymbol{e} + \boldsymbol{b}\boldsymbol{u} \qquad (11)$$

Equation (11) represents a linear time-invariant, single-input dynamic system, where $\boldsymbol{u} = -\boldsymbol{k}\boldsymbol{e}$ plays the role of a state feedback. Since (7) is the controllability matrix of (11), if (7) is full rank all the eigenvalues of (11) are controllable, i.e., they can be placed anywhere by proper vector $\boldsymbol{k}$ [6]. It can be concluded that (6) becomes a global observer of (5), provided that the eigenvalues of $(\boldsymbol{A} - \boldsymbol{b}\boldsymbol{k})$ lie in the open left half plane. ∘

Now it is *proved* that the plaintext can be retrieved from the ciphertext using the key $\tilde{K}(t) = K(\hat{\boldsymbol{x}}(t))$ generated by the decrypter (6).

Proposition 2: Let

$$\tilde{e}_{en}(t) = z - f(\hat{\boldsymbol{x}}) - \boldsymbol{k}\hat{\boldsymbol{x}} \qquad (12)$$

be the ciphertext recovered by the decrypter, and let

$$\tilde{p}(t) = d(\tilde{e}_{en}(t), \tilde{K}(t)) \qquad (13)$$

be the plaintext retrieved using $\tilde{e}_{en}(t)$ and $\tilde{K}(t)$. If (6) is a global observer of (5), it results:

$$\tilde{p}(t) \to p(t) \qquad (14)$$

Proof: If (6) is a global observer of (5), then $\hat{\boldsymbol{x}}(t) \to \boldsymbol{x}(t)$ for any initial condition. As a consequence, $K(\hat{\boldsymbol{x}}(t)) \to K(\boldsymbol{x}(t))$, that is, $\tilde{K}(t) \to K(t)$. Moreover, from (9) and (12) it follows that $\tilde{e}_{en}(t) \to e_{en}(t)$. Finally, the comparison between (3) and (13) clearly shows that (14) holds. ∘

The approach developed in this paper is based on *linear* observer, whereas the technique illustrated in [5] exploits *nonlinear* observer. As a consequence, it is worth noting that herein equation (6) represents a linear system *driven* by

the hyperchaotic signal (9), whereas in [5] the concept of *synchronization* between identical drive-response systems is considered.

3. EXAMPLE

The theoretical framework is now applied to design a cryptosystem based on hyperchaos. The circuit considered herein (described by (1)) is a 4th order hyperchaotic oscillator [4]:

$$\begin{aligned}\dot{x}_1 &= 0.7\,x_1 - x_2 - x_3\\ \dot{x}_2 &= x_1\\ \dot{x}_3 &= 3(x_1 - x_4)\\ \dot{x}_4 &= 3x_3 - 30(x_4 - 1)H(x_4 - 1)\end{aligned} \tag{15}$$

where $H()$ is the Heaviside function. The transmitter consists of system (15) and an encryption function $e_{en}(t)$. In particular, an *n*-shift cipher [1] is chosen for the encryption:

$$e_{en}(t) = f_1\left(\cdots f_1\left(f_1\left(p(t), K(t)\right), K(t)\right), \cdots, K(t)\right) \tag{16}$$

$$f_1(x, K) = \begin{cases} (x+K) + 2h & -2h \le (x+K) \le -h, \\ (x+K) & -h < (x+K) < h, \\ (x+K) - 2h & h \le (x+K) \le 2h \end{cases} \tag{17}$$

where (17) is recursively used for the encryption, h and n are cipher parameters, $K(t)$ is the chaotic key whereas $p(t)$ is the information signal. These parameters have been chosen as: $p(t) = 0.5\sin t$, h=4, n=30 and $K(t) = x_2(t)$. The transmitter described by (5) assumes the form:

$$\begin{aligned}\dot{x}_1 &= 0.7\,x_1 - x_2 - x_3\\ \dot{x}_2 &= x_1\\ \dot{x}_3 &= 3(x_1 - x_4)\\ \dot{x}_4 &= 3x_3 - 30(x_4 - 1)H(x_4 - 1) - 30e_{en}(t)\end{aligned} \tag{18}$$

By taking into account that the matrix (7) (derived from (15)) is full rank, it follows that the eigenvalues of (11) can be placed, for instance, in $\{-0.5 \mp 3.486\,j,\ -0.5 \mp 0.8222\,j\}$ for $k_1 = -3.6937$, $k_2 = 0.2445$, $k_3 = 1.0727$ and $k_4 = -2.7000$. As a consequence, the signal (9) transmitted over the channel becomes:

$$\begin{aligned} z(t) = {} & (x_4 - 1)H(x_4 - 1) - 3.6937x_1 + 0.2445x_2 \\ & + 1.0727x_3 - 2.7000x_4 + e_{en}(t) \end{aligned} \tag{19}$$

where the signal:

$$\begin{aligned} \bar{z}(t) = {} & (x_4 - 1)H(x_4 - 1) - 3.6937x_1 + 0.2445x_2 \\ & + 1.0727x_3 - 2.7000x_4 \end{aligned} \tag{20}$$

plays the role of a hyperchaotic masking signal. Namely, it is able to mask the encrypted signal $e_{en}(t)$, which in turn hides the message signal $p(t)$ (see Fig. 1). The receiver is designed as a *linear* observer for the state of the transmitter:

$$\begin{aligned}\dot{\hat{x}}_1 &= 0.7\,\hat{x}_1 - \hat{x}_2 - \hat{x}_3\\ \dot{\hat{x}}_2 &= \hat{x}_1\\ \dot{\hat{x}}_3 &= 3(\hat{x}_1 - \hat{x}_4)\\ \dot{\hat{x}}_4 &= 3\hat{x}_3 - 30z(t)\\ &\quad - 30(-3.6937\hat{x}_1 + 0.2445\hat{x}_2 + 1.0727\hat{x}_3 - 2.7\hat{x}_4)\end{aligned} \tag{21}$$

where $z(t)$ is the observed quantity. From (12) the encrypted signal recovered by the receiver is:

$$\begin{aligned} \hat{e}_{en}(t) = {} & z(t) - (\hat{x}_4 - 1)H(\hat{x}_4 - 1) \\ & - (-3.6937\hat{x}_1 + 0.2445\hat{x}_2 + 1.0727\hat{x}_3 - 2.7\hat{x}_4) \end{aligned} \tag{22}$$

By taking into account that the decryption rule is the same as the encryption one [1]:

$$p(t) = f_1\left(\cdots f_1\left(f_1\left(e_{en}(t), -K(t)\right), -K(t)\right), \cdots, -K(t)\right) \tag{23}$$

it follows that the recovered message signal is:

$$\hat{p}(t) = f_1\left(\cdots f_1\left(f_1\left(\hat{e}_{en}(t), -\hat{K}(t)\right), -\hat{K}(t)\right), \cdots, -\hat{K}(t)\right) \tag{24}$$

where $\hat{e}_{en}(t)$ is given by (22) whereas the key is generated by the receiver (21). By taking into account that the eigenvalues of (11) have been placed in the left plane, it results $\hat{\boldsymbol{x}}(t) \to \boldsymbol{x}(t)$. From (22) and (19) it follows that $\hat{e}_{en}(t) \to e_{en}(t)$. Moreover, the key $K(t) = x_2(t)$ generated by the transmitted tends toward the key $\hat{K}(t) = \hat{x}_2(t)$ generated by the receiver. From (23) and (24) it can be concluded that $\hat{p}(t) \to p(t)$ (see Fig. 2). Thus, by exploiting a system theory approach, it has been proved that the plaintext $p(t) = 0.5\sin t$ can be retrieved at the receiver *without transmitting any key over the channel.*

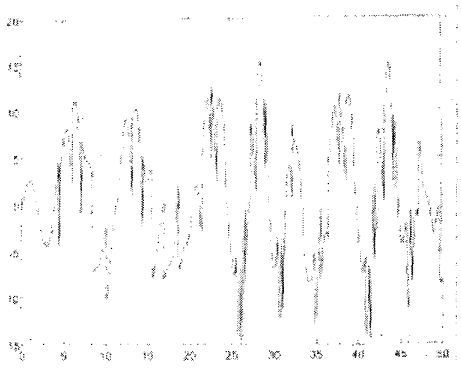

Fig. 1. Time waveform of the driving signal (19).

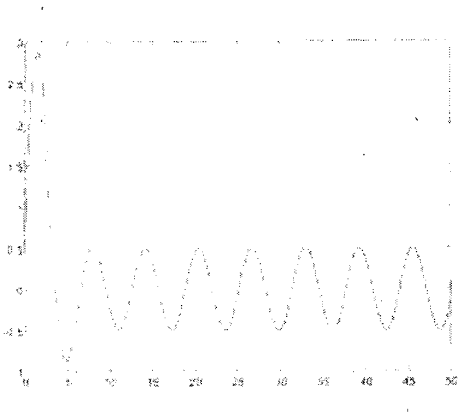

Fig. 2. Time waveform of the recovered signal (24).

4. DISCUSSION

- By computing the rank of (7) it can be easily shown that the encrypter (5) and the decrypter (6) can include several *hyperchaotic systems* (such as Rössler's system, the Matsumoto-Chua-Kobayashi circuit, its modified version and other hyperchaotic oscillators, see [5] for a survey).
- The security of a communications scheme can be enhanced by making the transmitted signal more complex [8]. In particular, in [7] it is suggested that two chaotic signals can be added together to create a carrier signal of sufficient complexity. In this way, it is not possible to predict the carrier dynamics based on a reconstruction of the geometric structure in the phase space [7]. The present paper makes a further contribution in this direction, since a transmitted signal of *high complexity* is used (for instance, see (19)).
- The forecasting approach developed in [7]-[8] enables the behavior of the chaotic carrier to be predict in low-dimensional systems. Although this is hard to do for hyperchaotic systems, consider the transmitted signal (19) and suppose that the carrier (20) is reconstructed in some way by an intruder. By considering the results available in literature, it seems that it is not possible for an intruder to reconstruct the key $x_2(t)$ starting from a completely different signal $\bar{z}(t)$. This *conjecture* leads to conclude that, even if the ciphertext $e_{en}(t) = z(t) - \bar{z}(t)$ is reconstructed, it is not possible for an intruder to obtain the plaintext $p(t)$. *Namely, taking into account that the key is not transmitted or reconstructed, it is not possible for an intruder to obtain the message, even if he is able to reconstruct in some way the encrypted signal.*
- The method illustrated herein and the one reported in [5] share the same advantages. Additionally, the present one is simpler, due to the adoption of *linear* observer.

ACKNOWLEDGMENT

This research is supported by Murst 40% (1998F).

5. REFERENCES

[1] YANG, T., WU, C. W., and CHUA, L. O.: "Cryptography based on chaotic systems", *IEEE Trans.*, 1997, **CAS-44**, (5), pp. 469-472.

[2] TAMASEVICIUS, A., MYKOLAITIS, G., CENYS, A., and NAMAJUNAS, A.: "Synchronization of 4D hyperchaotic oscillators", *Electron. Lett.*, 1996, **32**, (17), pp. 1536-1537.

[3] GRASSI, G., and MASCOLO, S.: "Nonlinear observer design to synchronize hyperchaotic systems via a scalar signal", *IEEE Trans.*, 1997, **CAS-44**, (10), pp. 1011-1014.

[4] TAMASEVICIUS, A., NAMAJUNAS, A., and CENYS, A.: "Simple 4D chaotic oscillator", *Electron. Lett.*, 1996, **32**, (11), pp. 957-958.

[5] GRASSI, G., and MASCOLO, S.: "A system theory approach for designing cryptosystems based on hyperchaos", *IEEE Trans.*, 1999, **CAS-46**, (9), pp. 1135-1138.

[6] BROGAN, W. L.: "Modern control theory" (Prentice-Hall, New Jersey, 1991).

[7] SHORT, K. M.: "Steps toward unmasking secure communications", *Int. J. Bifurcation Chaos*, 1994, **4**, (4), pp. 959-977.

[8] SHORT, K. M.: "Unmasking a modulated chaotic communications scheme", *Int. J. Bifurcation Chaos*, 1996, **6**, (2), pp. 367-375.