CHAOTIC DYNAMICS APPLIED TO CRYPTOGRAPHY

V. GUGLIELMI [1], D. FOURNIER-PRUNARET [1]
A.K. TAHA [1], P. PINEL [1], L. BENETEAU [2]

[1] LESIA (Laboratoire d'Etudes des Systèmes Informatiques et Automatiques)
[2] LAG (Laboratoire d'Arithmétique et de Géométrie des codes)
INSA, 135 Avenue de Rangueil, 31077 Toulouse Cedex 04, France
veronique.guglielmi@insa-tlse.fr, http://www.lesia.insa-tlse.fr

Abstract

In this paper, we propose different ways of using for encryption a two-dimensional noninvertible map presenting chaotic dynamics. We consider chaotic attractors as pseudo-random bit generators, to produce long, non-repeating, random-like sequences from a short key. In this kind of applications, the keystreams are some trajectories of the map, whereas the cipher key is given by the parameter values and the initial conditions, and we detail different possibilities to mix the keystream with the plaintext to produce the ciphertext. The inherent nonlinearity of chaos, associated to the important sensitivity to initial conditions, might guarantee the system security.

1. Chaotic Signals

Chaotic signals may be generated by physical non-linear circuits described by a set of parameters. Depending on the values of the parameters, the dynamics of these systems [1] can change drastically, exhibiting periodic, pseudo-periodic or chaotic waveforms - i.e. non-periodic deterministic processes, yet qualitatively very similar to random noise -. Then, chaotic attractors can be thought of as pseudo-random generators : given the sensibility to initial conditions, we may consider a chaotic sequence as one realization of a discrete stochastic process [3]. This will allow us to propose in the next section different kinds of discrete-time cryptosystems based on noninvertible maps.

But, to ensure security, an important point is the choice of the chaotic maps : the sequences must have good distribution properties for cryptography [4][5]. To obtain trajectories with right characteristics, we choose the chaotic sequences according to previous theoretical non linear dynamical results. For example, to have more secure cryptosystems, we can use chaotic signals with a relatively simple "macroscopic" evolution (cyclic for example), and of course an effective one much more complex.

It appears that several two-dimensional noninvertible maps may be convenient ; we will present in this paper only the following cubic one, where (x,y) are real variables, and a and b real parameters :

$$\begin{cases} x_{n+1} = y_n \\ y_{n+1} = a\left(-x_n{}^3 + x_n\right) + b\left(-y_n{}^3 + y_n\right) \end{cases}$$

For this map, the evolution of attractors and their basins (i.e. the set of initial conditions giving rise to iterated sequences converging towards the considered attractor) has been studied and is thoroughly explained in [2].

For example, when a = 2.2 and b = -0.99, a non-cyclic chaotic attractor exists and can be observed in the phase plane of figures 1 and 2.

Sensibility to initial conditions is the primary reason that the signals coming up in noninvertible maps may be considered as "random", and therefore may be applied to cryptography.

To illustrate this sensibility, let us consider two different sets of initial conditions, $(x_0 = 0.5, y_0 = -0.5)$ and $(x_0 = 0.3, y_0 = -0.3)$ for the examples presented in figures 1 and 2. They lead to sequences (x_n, y_n) and (x'_n, y'_n) apparently similar, as soon as the initial values are taken in the basin of a single attractor. Nevertheless, these two trajectories prove to always differ at least of 10^{-5}.

By definition of chaos, the sequences will evolve in the same way and will be similar from a qualitative point of view, but they will also verify $x'_n \neq x_n$ for each nth instant.

Furthermore, to have a still more secure cryptosystem, it is attractive to choose chaotic signals that seem to evolve simply. For our example, the attractor presented here is not cyclic : x_n does not evolve periodically from one domain of the phase plane to another, as demonstrated by figure 3 where only the points (x_n,y_n) with odd indices n are represented.

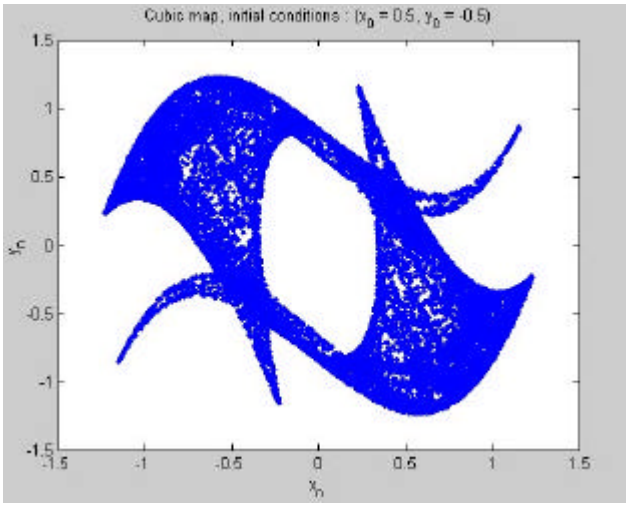

Fig.1 : Phase plane (x_n,y_n) – Cubic map, initial conditions : $(x_0 = 0.5, y_0 = -0.5)$

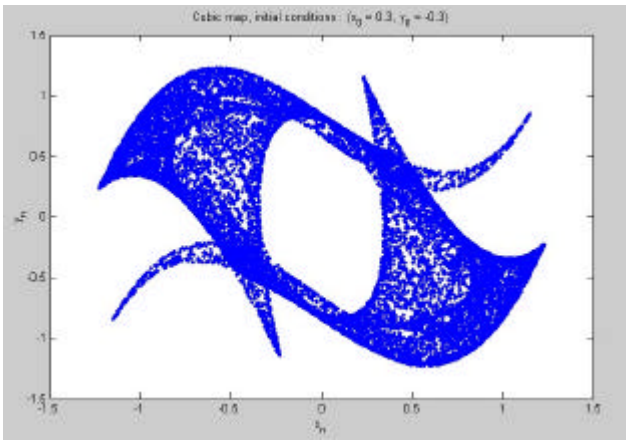

Fig.2 : Phase plane (x_n,y_n) – Cubic map, initial conditions : $(x_0 = 0.3, y_0 = -0.3)$

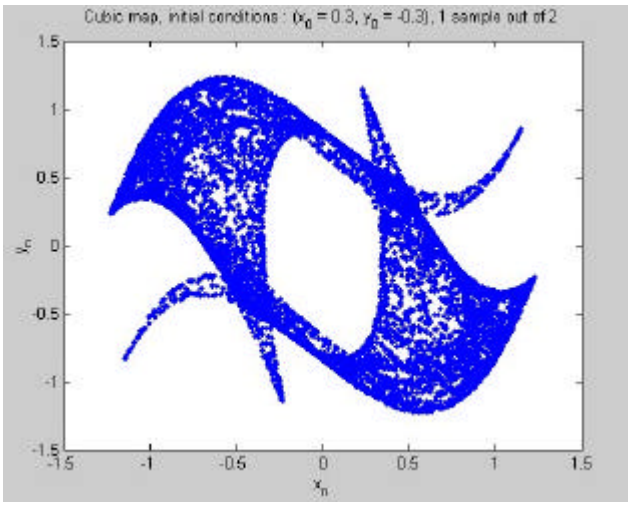

Fig.3 : Phase plane (x_n,y_n) – Cubic map, 1 sample out of 2

Nevertheless, the sequence x_n (and the corresponding keystreams) looks like a pseudo-periodic signal of period 2, as shown by the frequency content of the chaotic signal.

To describe the spectral components, we consider the chaotic sequence x_n as one realization of a stationary discrete random process, and we estimate the Power Spectral Density (PSD) of the process, using the popular non-parametric Welch's method (averaged periodograms of windowed signal sections). And, when we restrict initial conditions to the basin of a single attractor, it seems reasonable to assume that the process is stationary (even if it is not always true as we could have seen [3], depending on the type of chaotic map).

So, in figure 4, the plot of the estimated real-valued PSD shows the spectrum of x_n, at positive frequencies only (since x_n is always real), in decibels, versus normalized frequency.

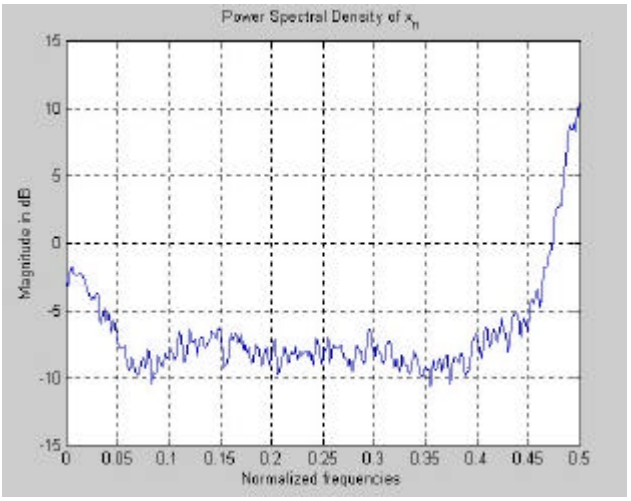

Fig.4 : PSD of x_n – Cubic map

Then, the PSD of x_n exhibits a peak at $f = 0.5$, leading to consider x_n as a periodic signal, of period 2, embedded in additive white noise.

The spectral peak at $f = 0$ doesn't exist because the two alternative values of x_n are opposite.

Note that this period 2 is related to an order 2 cyclic chaotic attractor which arises when b increases to the value -0.61 [2].

2. Encryption Laws

We suppose that the plaintext $\{p_n\}$ is in binary form, without attaching ourselves to the conversion which has led to this binary representation (because this previous step

seems to be independent from the performances of the cryptosystem itself).

Let us consider a noninvertible map F leading to chaotic sequences $\{s_n\}$. For our systems, we have chosen two-dimensional maps (like the cubic one described in the previous section), and we take for the chaotic sequence $\{s_n\}$ one of the two coordinates (x_n,y_n). To simplify the notations, we shall note for the chaotic point at nth instant : $s_n = F^n(s_0)$, where s_0 stands for the initial condition.

In the cryptographic discrete-time schemes explained below, the keystreams are some trajectories of the map, and we present three different possibilities to mix the keystream with the plaintext to produce the ciphertext. Note that these three laws can be used alone or associated to realize a more secure system. For the moment, we study independently the performances of each algorithm [6].

Anyway, the key of the cipher is constituted by both the parameter values and the initial conditions of the map.

Of course, using the initial conditions and the parameter values of the recurrence as the key implies that both the encryption system and the decryption system know them : the keystream is always supposed to be known for decryption. So the decryption system must be able to produce exactly the same chaotic sequences than the encryption system.

But all cryptographic schemes proposed here will be easy to implement because the transmission of a message does not need synchronization between emitter and receiver : each system will calculate the chaotic sequences independently, the initial conditions and the parameter values being given by a protocol of private and public keys. This permits us to avoid the problem of chaos synchronization.

Another advantage is that, although each key is short (the initial conditions and the parameter values), a very great number of different keys will exist.

Nevertheless, we noticed that the inherent nonlinearity of F, even associated to the important sensitivity to initial conditions, does not guarantee the security of the system : knowing a certain part of the chaotic sequence $\{s_n\}$ might allow an attacker to recover the whole keystream.

So, to increase security performances, we choose to transmit, for each real value s_n of a chaotic trajectory, not the whole binary representation of the chaotic point, but only certain bits of the representation. For that reason, it will be more difficult for an attacker to recover the keystreams.

To optimize both cipher security and transmission data rate, the transmitted bits for each real chaotic value s_n must represent the information sufficient for the receiver to determine to which trajectory belongs the corresponding real-valued point (to be able to perform decryption of the corresponding plaintext bit p_n).

And note that the mask defining the transmitted bits of the binary representation can be considered as being part of the communication key (like the initial conditions and the parameter values).

2.1 Using one chaotic signal

This method, coming out from the very well-known method of feedback shift registers [7], is to add mod-2 (XOR) the plaintext bits $\{p_n\}$ with the keystream $\{s_n\}$, also represented in binary form, to produce the ciphertext $\{c_n\}$ at each nth instant :

$$p_n \oplus s_n = c_n$$

Because the XOR operation is self-inverse, deciphering is carried out in the same way :

$$c_n \oplus s_n = (p_n \oplus s_n) \oplus s_n = p_n \oplus 0 = p_n$$

Here, we use for the keystream $\{s_n\}$ the successive points of a chaotic trajectory : each value given by the map being real, it is coded on binary form to be represented in a digital system (the code itself depends on the digital processor used and on the implementation of the encryption law) ; then, some bits of this binary representation of the real-valued chaotic point are added modulo 2 to the plaintext bits p_n.

In so doing, we obtain for the keystream a pseudo-random sequence, non periodic, as long as the message and not to be reused (since following points of the trajectory will be used for the other messages).

2.2 Using two chaotic signals

Here, to exploit more fully the chaos properties, the security of the cipher relies no longer on the noninvertibility of the XOR operation but only on the difficulty to distinguish between two keystreams.

So, given two different keystreams $\{s_n\}$ and $\{t_n\}$, the transmitted nth value c_n is either s_n or t_n, according on the corresponding nth bit p_n of the message :

$$c_n = s_n \text{ if } p_n = 0 \text{ ; } c_n = t_n \text{ if } p_n = 1$$

Deciphering is then carried out by comparison of the ciphertext c_n to the values of the two keystreams :

$$p_n = 0 \text{ if } c_n = s_n \text{ ; } p_n = 1 \text{ if } c_n = t_n$$

We use two trajectories of the same chaotic attractor for the ciphering sequences : $s_n = F^n(s_0)$ and $t_n = F^n(t_0)$, where s_0 and t_0 are two different initial conditions chosen in the basin of the same chaotic attractor. By definition of chaos, the values taken by the sequences $\{s_n\}$ and $\{t_n\}$ would be very close, and equally distributed. But, in the same time, s_n will never be equal to t_n !

Of course, as we still work on digital systems, the real values s_n and t_n are represented in a binary form, and some bits of this binary representation of either s_n or t_n, are transmitted.

2.3 Using three chaotic signals

In order to ameliorate security and to increase the difficulty to distinguish between the two keystreams of the previous sub-section, we can also hide the transmitted information directly into chaos instead of using a part binary representation of the transmitted values.

So, let us consider now three trajectories of the same map leading to chaos : $s_n = F^n(s_0)$, $t_n = F^n(t_0)$ and $z_n = F^n(z_0)$, where s_0, t_0 and z_0 are three different initial conditions.

The transmitted nth value c_n is :

$$A_n = [s_n + z_n] \text{ if } p_n = 0 \text{ ; } B_n = [t_n + z_n] \text{ if } p_n = 1$$

where p_n is the corresponding nth bit of the message.

At the receiver, deciphering is carried out after subtraction of z_n, by comparison of the ciphertext c_n to the values of the two keystreams s_n and t_n.

3. Conclusions

Thinking of chaos as a pseudo-random generator, we proposed different ways to use chaotic signals for encryption. For chaotic sequences permit to build long and non repeating keystreams.

But, as we consider digital cryptosystems, the real-valued chaotic points are somehow quantized : only a finite number of values can be represented. So, when the message length become greater than the number of different values, the keystream will be periodic.

Then, the question is more generally to evaluate the precision needed to preserve chaos properties within a digital scheme, as well as the computation time following from it.

To do so and to determine security performances, we are implementing by now the actual realization of the proposed algorithms, with Digital Signal Processors (DSP) as DSP are highly efficient to perform discrete calculus.

---

[1] C. Mira, L. Gardini, A. Barugola, J.C. Cathala, « Chaotic dynamics in two-dimensional noninvertible maps », *World Scientific*, Series A, Vol. 20, 636 pages, juin 1996.

[2] D. Fournier-Prunaret & V. Guglielmi, "Bifurcations and attractors in two-dimensional maps of cubic type", *NOLTA'99*, Hawaï (USA), 29 Nov. - 2 Dec. 1999.

[3] V. Guglielmi, D. Fournier-Prunaret, G. Kolumban & Z. Jako, "Composantes spectrales du chaos", *Gretsi 2001*, Toulouse (France), September 2001.

[4] L. Kocarev, "Chaos-based cryptography: a brief overview", *IEEE Circuits & Systems Magazine*, vol. 1, no. 3, 2001.

[5] N. Masuda & K. Aihara, "Cryptosystems with discretized chaotic maps", *IEEE Trans. on Circuits and Systems I: Fundamental Theory and Applications*, vol. 49, no. 1, January 2002.

[6] L. Bénéteau, D. Fournier-Prunaret, V. Guglielmi, P. Pinel, S. Rouabhi & A.K. Taha, "Two encryption schemes using the chaotic dynamics of two-dimensional noninvertible maps", *NDES'02 The Nonlinear Dynamics of Electronic Systems*, Izmir (Turquie), 21 - 23 June 2002 (published in the Complements to Proceedings).

[7] Diffie & Hellman, "An introduction to cryptography", *Proceedings of the IEEE*, vol. 67, no. 3, March 1979.