Available online at www.sciencedirect.com
SCIENCE DIRECT®
Chaos, Solitons and Fractals 21 (2004) 1265–1269
CHAOS SOLITONS & FRACTALS
www.elsevier.com/locate/chaos

Cryptography with chaos at the physical level

Romuel F. Machado [a,*], Murilo S. Baptista [b], C. Grebogi [b]

[a] Departamento de Física, Universidade Federal de Ouro Preto, Campus Morro do Cruzeiro, Ouro Preto-MG 35400, Brazil
[b] Instituto de Física, Universidade de São Paulo, P.O. Box 66318, São Paulo, SP 053150-970, Brazil

Accepted 12 December 2003

Abstract

In this work, we devise a chaos-based secret key cryptography scheme for digital communication where the encryption is realized at the physical level, that is, the encrypting transformations are applied to the wave signal instead to the symbolic sequence. The encryption process consists of transformations applied to a two-dimensional signal composed of the message carrying signal and an encrypting signal that has to be a chaotic one. The secret key, in this case, is related to the number of times the transformations are applied. Furthermore, we show that due to its chaotic nature, the encrypting signal is able to hide the statistics of the original signal.

In this letter, we present a chaos-based cryptography scheme designed for digital communication. We depart from the traditional approach where encrypting transformations are applied to the binary sequence (the symbolic sequence) into which the wave signal is encoded [1]. In this work, we devise a scheme where the encryption is realized at the physical level, that is, a scheme that encrypts the wave signal itself.

Our chaos-based cryptographic scheme takes advantage of the complexity of a chaotic transformation. This complexity is very desirable for cryptographic schemes, since security increases with the number of possibilities of encryption for a given text unit (a letter for example). One advantage of using a chaotic transformation is that it can be implemented at the physical level by means of a low power deterministic electronic circuit which can be easily etched on a chip. Another advantage is that, contrary to a stochastic transformation, a chaotic one allows an straightforward decryption. Moreover, as has been shown elsewhere [2], chaotic transformations for cryptography, enables one to introduce powerful analytical methods to analyze the method performance, besides satisfying the design axioms that guarantees security.

In order to clarify our goal and the scheme devised, in what follows, we initially outline the basic ideas of our method. Given a message represented by a sequence $\{y_i^0\}_{i=1}^{l}$, and a chaotic encrypting signal $\{x_i^0\}_{i=1}^{l}$, with y_i and $x_i \in \mathbb{R}$ and $x_{i+1} = G(x_i)$, where G is a chaotic transformation, we construct an ordered pair (x_i^0, y_i^0). The ith element of the sequence representing the encrypted message is the y component of the ordered pair (x_i^n, y_i^n), obtained from $F_c^n(x_i^0, y_i^0)$. The function $F_c : \mathbb{R}^2 \to \mathbb{R}^2$ is a chaotic transformation and n is the number of times we apply it to the ordered pair. The nth iteration of (x_i^0, y_i^0), has no inverse if n and x_i^0 are unknown, that is, y_i^0 can not be recovered if one knows only $F_c^n(x_i, y_i)$. As it will be clear further, this changing of initial condition is one of the factors responsible for the security of the method.

Now we describe how to obtain the sequence $\{y_i\}_{i=1}^{l}$ by means of the sampling and quantization methods. These methods play an essential role in the field of digital communication, since they allow us to treat signals varying continuously in time as discrete signals. One instance of the use of continuous in time signals is the encoding of music or

* Corresponding author.
E-mail address: romuelm@iceb.ufop.br (R.F. Machado).

0960-0779/$ - see front matter © 2004 Elsevier Ltd. All rights reserved.
doi:10.1016/j.chaos.2003.12.094

speech where variations in the pressure of the air are represented by a continuous signal such as the voltage in an electric circuit. In the *sampling* process, a signal varying continuously in time is replaced by a set of measurements (samples) taken at instants separated by a suitable time interval provided by the sampling theorem [3,4]. The signals to which the sampling theorem applies are the band limited ones. By a band limited signal, we mean a function of time whose Fourier transform is null for frequencies f such that $|f| \geqslant W$. According to the sampling theorem, it is possible to reconstruct the original signal from samples taken at times multiple of the sampling interval $T_S \leqslant 1/2W$. Thus, at the end of the sampling process, the signal is converted to a sequence $\{s_1^0, s_2^0, \ldots, s_l^0\}$ of real values, which we refer to as the s sequence. After being sampled the signal is *quantized*. In this process, the amplitude range of the signal, say the interval $[a,b]$, is divided into N subintervals $\mathscr{R}_k = [a_k, a_{k+1})$, $1 \leqslant k \leqslant N$, with $a_1 = a$, $a_{k+1} = a_k + \delta_k$, $a_{N+1} = b$, where δ_k is the length of the kth subinterval. To each $\mathscr{R}_k$ one assigns an appropriate real amplitude value $q_k \in \mathscr{R}_k$, its middle point for example. A new sequence, the y sequence, is generated by replacing each s_i^0 by the q_k associated to the $\mathscr{R}_k$ region to which it belongs. So, the y sequence $\{y_1^0, y_2^0, \ldots, y_l^0\}$ is a sequence where each $y_i^0 \in \mathbb{R}$ takes on values from the set $\{q_1, \ldots, q_N\}$. In traditional digital communication, each member of the y sequence is encoded into a binary sequence of length $\log_2 N$. Thus, traditional cryptographic schemes, and even recent proposed chaotic ones [1], transforms this binary sequence (or any other discrete alphabet) into another binary sequence, which is then modulated and transmitted. In our proposed scheme, we transform the real y into another real value, and then modulate this new y value in order to transmit it. This scheme deals with signals rather than with symbols, which implies that the required transformations are performed at the hardware or physical level. Instead of applying the encrypting transformations to the binary sequence, we apply them to the y^0 sequence, the sequence obtained by sampling and quantizing the original wave signal.

Suppose, now, that the amplitude of the wave signal is restricted to the interval [0,1]. The first step of the process is to obtain the encrypting signal, a sequence $\{x_1^0, x_2^0, \ldots, x_l^0\}$, $0 < x_i^0 < 1$. As we will show, this signal is obtained by either sampling a chaotic one or by a chaotic mapping. The pair (x_i^0, y_i^0) localizes a point in the unit square. In order to encrypt y_i^0, we apply the baker map to the point (x_i^0, y_i^0) to obtain $(x_i^1, y_i^1) = (2x_i^0 - \lfloor 2x_i^0 \rfloor, 0.5(y_i^0 + \lfloor 2x_i^0 \rfloor))$, where $\lfloor 2x_i^0 \rfloor$ is the largest integer equal to or less than $2x_i^0$. The encrypted signal is given by y_i^1, that is, $0.5(y_i^0 + \lfloor 2x_i^0 \rfloor)$. It is important to notice that y_i^1 can take $2N$ different values instead of N, since each y_i^0 may be encoded as either $0.5 * (y_i^0) < 0.5$ or $0.5 * (y_i^0 + 1) > 0.5$, depending on whether x_i^0 falls below or above 0.5. So, in order to digitally modulate the encrypted signal for transmission, $2N$ pulse amplitudes are necessary, with each binary block being encoded by two different pulses. Therefore, our method has an output format that can be straightforwardly used in digital transmissions. Suppose, for example, that $N = 2$, and we have $q_1 = 0.25$ and $q_2 = 0.75$. If $s_i^0 < 0.5$ then $y_i^0 = 0.25$ and if we use $n = 1$, we have $y_i^1 = 0.125$ if $x_i^0 < 0.5$ or $y_i^1 = 0.625$ if $x_i^0 \geqslant 0.5$. On the other hand, if $s_i^0 > 0.5$, then $y_i^0 = 0.75$ and we have $y_i^1 = 0.375$, if $x_i^0 < 0.5$ or $y_i^1 = 0.875$ if $x_i^0 \geqslant 0.5$. So, the encrypted signal takes on values from the set $\{0.125, 0.375, 0.625, 0.875\}$, where the first and third values can be decrypted as 0.25 in the non-encrypted signal while the second and the forth as 0.75. In a general case, where we apply n iterations of the mapping, y_i^1 can assume $2^n N$ different values. In this case, if one wants to digitally transmit the cipher text, one can encode every cipher text unit using a binary block of length $\log_2(2^n N)$ and then modulate this binary stream using $2^n N$ pulse amplitudes. Thus, the decryption is straightforward if one knows how many times the baker map was applied during the encryption.

If the baker transformation (function F_c) is applied n times, there are, for each plain text unit, $2^n N$ possible cipher text units. In this case, the complexity of the ciphertext, that is, its security, can have its upper bound estimated by the Shannon complexity H_s which is the logarithm of the possible number of ciphertext units, produced after the baker's map have been applied n times. So, $H_s = n\log(2) + \log(N)$. We see that n is much more important for security reasons than N. So, if one wishes to improve security, one could implement a dynamical secret key schedule for n. By this we mean that, based on some information of the encrypted trajectory (x_i^1, y_i^1), the value of n could be changed whenever a plain text unit is encrypted. If one allows only m values for n, the number of possible cipher text units would be given by $N^m \prod_{j=1}^{m} 2^{n_j}$ and the complexity of the cipher text would be $\sum_{j=1}^{m} n_j \log 2 + m \log N$, which can be very high, even for small m. Thus, without knowing the number n of applications of the baker map during the encryption, the decryption renders highly improbable. In fact, n is the secret key of our cryptographic scheme and we can think of the sequence $\{x_i^0\}$ as a dynamical secret key schedule for the x-component in the initial condition represented by the ordered pair (x_i^0, y_i^0).

The tools necessary to perform the security analysis are provided by the information theory. In this context, information sources are modelled by random processes whose outcome may be either discrete or continuous in time. Since major interest, and ours too, is in band limited signals, we restrict ourselves to the discrete case, where the source is modelled by a discrete time random process. This is a sequence $\{y_i^0\}_{i=1}^{l}$ in which each y_i^0 assumes values within the set $\mathscr{A} = \{q_1, q_2, \ldots, q_N\}$. This set is called the alphabet and its elements are the letters. To each letter is assigned a probability mass function $p(q_j) = P(y_i^0 = q_j)$, that gives the probability with which the letter is selected for transmission.

In cryptography, one deals with two messages: the plain text $\{y_1^0, y_2^0, \ldots, y_l^0\}$ and the encrypted or cipher text $\{y_1^1, y_2^1, \ldots, y_l^1\}$, where y_i^1 assumes values from the same set $\mathscr{A}$ if N levels are used in quantizing the incoming signal. A secure cryptographic scheme must be such that no information about the plain text can be obtained from the cipher text. This requirement is quantified by means of the mutual information $I(y^0; y^1)$ [5,6], which is defined as

$$I(y^0; y^1) = \sum_{i,j} p(q_i, q_j) \log \frac{p(q_i, q_j)}{p(q_i)p(q_j)}, \tag{1}$$

where $p(q_i, q_j)$ is the joint probability of occurrence of q_i in the plain text and q_j in the cipher text. This probability may be written as

$$p(q_i, q_j) = p(q_i)p(q_j|q_i), \tag{2}$$

where $p(q_j|q_i)$ is the conditional probability that q_i in the plain text is encrypted as q_j in the cipher text. Perfect security, according to Shannon, means $I(y^0; y^1) = 0$, which implies $p(q_i, q_j) = p(q_j)p(q_i)$, that is $p(q_j|q_i) = p(q_j)$ or $p(q_i|q_j) = p(q_i)$. Thus, perfect security is guaranteed if the plain text and cipher text are statistically independent [5], that is, given a q_i in the plain text it may be encrypted as any letter in $\mathscr{A}$ with a uniform probability distribution. It must be so if one wishes to prevent the statistics of the plain text from being present in the cipher text. Indeed, security in our scheme is based on the fact that chaotic systems have an invariant probability density, which implies that whatever is the type of message being encrypted by the chaotic transformation, the encrypted text presents only statistical properties of the public chaotic transformation.

Note that increasing the number of iterations n by m, the number of elements in the alphabet of the ciphertext is increased by 2^m. For n sufficiently large and $n \gg N$, these elements can be understood as a coarse graining of the domain $[0, 1]$ of the Bernoulli shift, and the probability function of this discrete set is then approximately equal to the invariant probability density of the Bernoulli shift. Therefore, for large n, an encrypted letter y_i^n of the ciphertext is independent of the next letter y_{i+1}^n, likewise the nth iterate of a point, by the Bernoulli shift, is independent of this point.

If, for example, we use $N = 2$ quantization levels, and restrict the signal amplitude range to the interval $(0, 1)$, $s_i^0 < 0.5$ gives $y_i^0 = q_1$ while $s_i^0 \geqslant 0.5$ gives $y_i^0 = q_2$. The encrypted value $0.5 * (y_i^0 + \lfloor 2x_i^0 \rfloor)$, after quantization at the receiver, represents a q_1 if $x_0 < 0.5$ or a q_2 otherwise. If the encrypting signal $\{x_1^0, x_2^0, \ldots, x_l^0\}$ is identically and uniformly distributed (over the interval $[0, 1]$), then the encrypted values y_i^1 will be decoded at the receiver as either q_1 or q_2 with the same probability, independently of the letter represented by y_i^0. Although we have used $N = 2$ and $n = 1$ as example, the above analysis is valid for any N and any n. The security of the method depends only on the statistical properties of the encrypting signal and on the fact that the cryptanalyst does not know n, the number of times the baker transformation is applied during the encrypting process, even if this process is known.

An encrypting sequence satisfying the requirements for perfect security can be obtained by a chaotic mapping. Consider, for example, the Bernoulli shift defined as

$$x_{i+1}^0 = 2x_i^0 - \lfloor 2x_i^0 \rfloor. \tag{3}$$

To illustrate how the statistics of the plain text is hidden by the encrypting signal, we consider as the sampled signal, the constant sequence $s_i^0 = 0.1$ for $i = 1, \ldots, l$. In this case, the corresponding y^0 sequence is a sequence of q_1s for $N = 2$. The encrypted sequence is shown in Fig. 1. The values 0.125 and 0.625 are the values that y_i^1 takes on. These values are replaced by q_1 and q_2, respectively, if the $N = 2$ levels are used by the receiver in quantizing the incoming analog signal. Thus, the cipher text looks like a random sequence in which q_1s and q_2s appear with the same frequency, which is totally different, in statistical terms, from the message to be encrypted that is formed by the constant sequence. Due to the chaotic character of the encrypting signal, any encrypted sequence has this character too, independently of the characteristics of the original sequence.

The chaotic dynamical system we used to generate the encrypting signal, the Bernoulli shift, is an idealized one. In order to implement the cryptographic system herein introduced, we use as encrypting signal, a chaotic one generated by a physical process. The Lorenz system [7,8], given by $\mathrm{d}x/\mathrm{d}t = \sigma(y - x)$, $\mathrm{d}y/\mathrm{d}t = rx - xz - y$ and $\mathrm{d}z/\mathrm{d}t = xy - bz$ fulfills this task, since these equations model the behavior of electric circuits, where the signals $x(t)$, $y(t)$ and $z(t)$ represent voltages [9]. For the parameter values $\sigma = 10$, $b = 8/3$ and $r = 28$, the Lorenz system exhibits chaotic behavior. Using these values for the parameters and the initial conditions $x(0) = 10.0$, $y(0) = 0.0$ and $z(0) = 5.0$, we take samples of $y(t)$, 1 unit of time apart starting at $t = 20$, in order to obtain the encrypting signal. The result of using this sampled signal as the encrypting one for the y sequence $y_i^0 = 0.1$ is shown in Fig. 2. Again, the constant in time signal is mapped into a seemingly random one, satisfying the requirements for perfect security.

Note that the presence of a finite correlation between x_i^0 and x_{i+1}^0 (both generated by the Lorenz system) does not imply a finite correlation between the encrypted signals y_i^n and y_{i+1}^n, since each of the encrypted signals y_i^n and y_{i+1}^n are

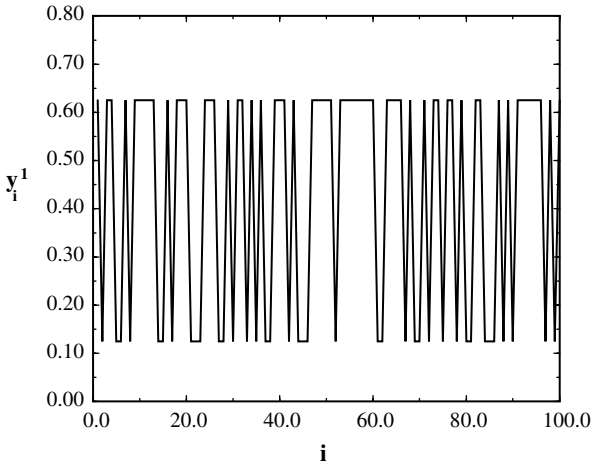

Fig. 1. Encrypted signal y_i^1 obtained by $n = 1$ iteration of the baker map (function F_c) applied to the ordered pair (x_i^0, y_i^0), where y_i^0 represents a constant message $y_i^0 = 0.25$ of length $l = 100$. We use the Bernoulli shift map to generate the encrypting signal x_i^0. Note that y_i^1 looks like a random sequence of two events, despite the fact that the message is constant.

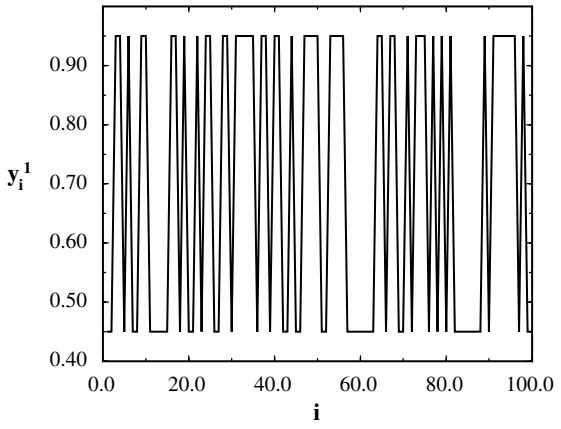

Fig. 2. Encrypted signal y_i^1 obtained by $n = 1$ iteration of the baker map (function F_c) applied to the ordered pair (x_i^0, y_i^0), where y_i^0 represents a constant message $y_i^0 = 0.25$ of length $l = 100$. We use a sampling of the $y(t)$ coordinate of the Lorenz system as the encrypting signal x_i^0. Note that y_i^1 looks like a random sequence of two events, despite the fact that the message is constant.

obtained by repeated iterations of the baker map and thus they can be seen as products of a pseudo-random number generator.

We have shown, that by taking advantage of the sampling and quantization techniques used in converting analog signals into digital ones, a secret key chaotic cryptographic scheme is accomplished. The encryption is realized at the physical level, that is, the encryption transformations are applied to the signal instead to the symbolic sequence. The secret key, in this case, is the number n of times a chaotic transformation is applied during the encryption. In addition, the resulting encrypted signal can be digitally transmitted. We have seen that the security of the system lies on the fact that the encrypting signal is a chaotic one, which implies that only its statistical properties are present in the encrypted text. This kind of signal can be obtained, for example, from electric circuits that are modelled by the Lorenz system, making feasible the implementation of the system.

A related issue is how noise affects the proposed scheme, since it seems to be noise sensitive for large values of N and n. In fact, as shown in [10], information encoded by chaotic signals are fully recovered when there is noise in the channel, and small parameter differences between the encoder and the decoder do not affect a full recovering of the information. This question, the related one concerning error correction devices, and how to improve the security of the method will be addressed in the future.

Acknowledgements

This work was supported by CNPq, FAPESP and FAPEMIG, brazilian funding agencies.

References

[1] Baptista MS. Cryptography with chaos. Phys Lett A 1998;240:50–3;
Alvarez G, Montoya F, Romera M, Pastor G. Cryptanalysis of a chaotic encryption system. Phys Lett A 2000;276:191–6;
Jakimoski G, Kocarev L. Logistic map as a block encryption algorithm. Phys Lett A 2001;289:199–206;
Jakimoski G, Kocarev L. Analysis of some recently proposed chaos-based encryption algorithms. Phys Lett A 2001;291:381–4;
Garcia P, Jiménez J. Communication through chaotic map systems. Phys Lett A 2002;298:35–40;
Wong KW. A combined chaotic cryptographic and hashing scheme. Phys Lett A 2003;307:292–8;
Wong KW. A fast chaotic cryptographic scheme with dynamic look-up table. Phys Lett A 2002;298:238–42.
[2] Götz M, Kelber K, Schwarz W. Discrete-time chaotic encryption systems. 1. Statistical design approach. IEEE Trans Circuit Systems I Fund Theory Appl 1997;44:963–70;
Dachselt F, Kelber K, Schwarz W. Discrete-time chaotic encryption systems—part III: Cryptographical analysis. IEEE Trans Circuit Systems I Fund Theory Appl 1998;45:983–8.
[3] Pierce JR. An introduction to information theory, symbols, signals and noise. New York: Dover; 1980.
[4] Proakis JG, Salehi M. Communication systems engineering. New Jersey: Prentice Hall; 2002.
[5] Haykin SS. Communication systems. New York: John Wiley & Sons; 2000.
[6] Cover TM, Thomas JA. Elements of information theory. New York: Wiley-Interscience; 1991.
[7] Lorenz EN. Deterministic non-periodic flow. J Atmos Sci 1963;20:130–41.
[8] Guckenheimer J, Holmes P. Nonlinear oscilations, dynamical systems, and bifurcation of vector fields. New York: Springer-Verlag; 1990.
[9] Cuomo KM, Oppenheim AV. Circuit implementation of synchronized chaos with applications to communications. Phys Rev Lett 1993;71:65–8.
[10] Rosa Jr E, Hayes S, Grebogi C. Noise filtering in communication with chaos. Phys Rev Lett 1997;78:1247–50;
Baptista MS, Lopez L. Information transfer in chaos-based communication. Phys Rev E 2002.