Available online at www.sciencedirect.com
SCIENCE DIRECT®
C. R. Mecanique 332 (2004) 969–972
COMPTES RENDUS MECANIQUE
http://france.elsevier.com/direct/CRAS2B/

Chaos synchronization on the N-torus and cryptography

Lionel Rosier [a], Gilles Millérioux [b], Gérard Bloch [b]

[a] *Institut Elie Cartan de Nancy, université Nancy 1, BP 239, 54506 Vandœuvre-lès-Nancy cedex, France*
[b] *Centre de recherche en automatique de Nancy, université Nancy 1, CRAN – ESSTIN, 2, rue Jean Lamour, 54519 Vandœuvre-les-Nancy, France*

Received 29 June 2004; accepted 2 September 2004

Available online 5 November 2004

Presented by Évariste Sanchez-Palencia

Abstract

A class of chaotic dynamical systems on the N-dimensional torus is proposed for masking some information in secure communications. The information is then recovered thanks to a chaos synchronization process. ***To cite this article: L. Rosier et al., C. R. Mecanique 332 (2004).***

Résumé

Synchronisation du chaos sur le tore N-dimensionnel et cryptographie. Nous proposons une classe de systèmes chaotiques sur le tore N-dimensionnel pour masquer une information à transmettre dans une communication sécurisée. Cette information est ensuite reconstruite à l'aide d'un mécanisme de synchronisation du chaos. ***Pour citer cet article : L. Rosier et al., C. R. Mecanique 332 (2004).***

Keywords: Control; Ergodicity; Chaos synchronization; Cryptography

Mots-clés : Automatique ; Ergodicité ; Synchronisation du chaos ; Cryptographie

1. Introduction

From the pioneering works reported in [1,2], information chaotic masking for private and secure communications has attracted much interest. Several works attempting to bring out a connection with conventional cryptography have revealed that not all chaotic maps are good candidates for encryption purposes (see [3]). Indeed, on one hand, from the sake of security, chaotic maps must produce signals which have no patterning, short correlation

E-mail addresses: rosier@iecn.u-nancy.fr (L. Rosier), millerioux@esstin.uhp-nancy.fr (G. Millérioux), bloch@esstin.uhp-nancy.fr (G. Bloch).

1631-0721/$ – see front matter
doi:10.1016/j.crme.2004.09.001

times and flat spectra. On the other hand, the cryptographic techniques must be compatible with an ease of design and implementation.

A cryptographic scheme must involve some classes of chaotic maps for which the dimension and the number of parameters can be arbitrarily large while computational requirements for masking and unmasking information must not be too heavy.

The aim of this note is to show that all these requirements are fulfilled for a large class of affine transformations of the N-dimensional torus.

2. Chaotic affine transformations of the N-torus

2.1. Affine transformations of the N-torus

Let $\mathbb{T}^N$ denotes the N-dimensional torus, i.e. $\mathbb{T}^N = \mathbb{R}^N/\mathbb{Z}^N$ (quotient vector space). For any $X=(X_1, \ldots, X_N) \in \mathbb{R}^N$, the class of X in $\mathbb{T}^N$ (namely the coset $X + \mathbb{Z}^N$) is denoted by $x = \overline{X}$. The distance between two points $\overline{X}$, $\overline{Y}$ is defined as $d(\overline{X}, \overline{Y}) = \inf_{Z\in\mathbb{Z}^N} |X - Y + Z|$.

For any matrix $M \in \mathbb{Z}^{P\times N}$ ($P, N \geqslant 1$) and for any $X \in \mathbb{R}^N$, the class of MX in $\mathbb{T}^P$, which clearly depends only of $\overline{X}$, will be denoted by $M\overline{X}$. We may associate to any matrix $A \in \mathbb{Z}^{N\times N}$ and to any $b \in \mathbb{T}^N$ a discrete dynamical system on $\mathbb{T}^N$ defined as

$$(\Sigma_{A,b}) \quad \begin{cases} x_{k+1} = f(x_k) := Ax_k + b, \\ x_0 \in \mathbb{T}^N \end{cases} \tag{1}$$

The map f is called an *affine transformation* of the N-torus.

2.2. Chaotic systems

The following definition of a chaotic system is due to Devaney [4] (see also [5]).

Definition 2.1. The dynamical system $(\Sigma_{A,b})$ is said to be *chaotic* if the following conditions are fulfilled:

(C1) (*Sensitive dependence on initial conditions*) There exists a number $\varepsilon > 0$ such that for any $x_0 \in \mathbb{T}^N$ and any $\delta > 0$, there exists a point $y_0 \in \mathbb{T}^N$ with $d(x_0, y_0) < \delta$ and an integer $k \geqslant 0$ such that $d(x_k, y_k) \geqslant \varepsilon$.
(C2) (*One-sided topological transitivity*) There exists some $x_0 \in \mathbb{T}^N$ with $(x_k)_{k\geqslant 0}$ dense in $\mathbb{T}^N$.
(C3) (*Density of periodic points*) The set $D = \{x_0 \in \mathbb{T}^N;\ \exists k > 0,\ x_k = x_0\}$ is dense in $\mathbb{T}^N$.

The first result in this note characterizes the chaotic affine transformations of $\mathbb{T}^N$.

Theorem 2.2 [6]. *Let $A \in \mathbb{Z}^{N\times N}$ and $b \in \mathbb{T}^N$. Assume that 1 is not an eigenvalue of A. Then $(\Sigma_{A,b})$ is chaotic if, and only if,* $\det A \neq 0$ *and A has no roots of unity as eigenvalues.*

2.3. Equidistribution

Let us consider now a discrete dynamical system with some *output*

$$\begin{cases} x_{k+1} = Ax_k + b, \\ y_k = Cx_k \end{cases}$$

where $x_0 \in \mathbb{T}^N$, $y_k \in \mathbb{T}^1$, $A \in \mathbb{Z}^{N\times N}$, $b \in \mathbb{T}^N$ and $C \in \mathbb{Z}^{1\times N}$. It is expected (and desired, as the output has to convey the information through the channel) that the output y_k inherits the chaotic behavior of x_k. However, Devaney's

definition of a chaotic system cannot be tested on the sequence (y_k), since this sequence is not a trajectory of a dynamical system. Instead, we may give a condition ensuring that the sequence (y_k) is equidistributed [7] (hence dense) in $\mathbb{T}^1$ for a.e. x_0, a property which may be seen as an *ersatz* of (C2).

Theorem 2.3 [6]. *Let $A \in \mathbb{Z}^{N\times N}$, $b \in \mathbb{T}^N$ and $C \in \mathbb{Z}^{1\times N} \setminus \{0\}$. Assume that* $\det A \neq 0$ *and that A has no roots of unity as eigenvalues (hence $\Sigma_{A,b}$ is chaotic). Then for a.e. $x_0 \in \mathbb{R}^N$ the sequence (x_k) (defined in* (1)*) is equidistributed in $\mathbb{T}^N$, and the sequence $(y_k) = (Cx_k)$ is equidistributed in $\mathbb{T}^1$.*

The proof of Theorem 2.3 rests on some ergodicity property [8] for such affine transformations.

3. Chaos synchronization and cryptography

The aim of this section is to suggest a chaos-based encryption scheme resorting to the modulo maps presented in the previous section. It is well known that an encryption scheme must ensure both confusion and diffusion [3]. To this end, at each discrete time k the symbol u_k of a plaintext $(u_k)_{k\geqslant 0}$ is injected in a chaotic recursion. Besides, confusion is reinforced by a suitable output function acting as a mapping from a high dimensional state space to a low dimensional state space (e.g., of dimension 1).

A discrete dynamical system (at the encryption part) fulfilling the above requirements is as follows

$$(\Sigma) \quad \begin{cases} x_{k+1} = A(x_k + Mu_k) + b =: A\tilde{x}_k + b, \\ y_k = C\tilde{x}_k \end{cases}$$

Here $A \in \mathbb{Z}^{N\times N}$ $(N \geqslant 1)$, $C \in \mathbb{Z}^{1\times N}$, $M \in \mathbb{Z}^{N\times 1}$, $x_k \in \mathbb{T}^N$ is the state, $u_k \in \mathbb{T}^1$ is the input containing the information to be masked, and y_k is the output conveyed to the receiver through the channel. Let us turn to the synchronization problem. A rather natural attempt consists of selecting as a candidate observer for Σ the system

$$(\hat{\Sigma}) \quad \begin{cases} \hat{x}_{k+1} = A\hat{x}_k + L(y_k - \hat{y}_k) + b, \\ \hat{y}_k = C\hat{x}_k \end{cases}$$

where the Luenberger matrix L is chosen in $\mathbb{Z}^{N\times 1}$ (so that $\hat{x}_{k+1}$ is defined in a unique way in $\mathbb{T}^N$). As usual, $\hat{x}_0$ is an arbitrary point in $\mathbb{T}^N$.

Setting $e_k = x_k - \hat{x}_k (\in \mathbb{T}^N)$, the error dynamics reads

$$e_{k+1} = (A - LC)(\tilde{x}_k - \hat{x}_k) = (A - LC)(e_k + Mu_k) \tag{2}$$

The gain matrix L has then to be chosen in such a way that (i′) the spectrum of $A - LC$ lies in the set $\{z \in \mathbb{C}; |z| < 1\}$; (ii′) L is $\mathbb{Z}$-valued. This imposes some restrictions on the choice of the pair (A, C).

A pair $(A^\flat, C^\flat)$ is said to be in a *companion canonical form* if it takes the form

$$A^\flat = \begin{pmatrix} -\alpha_N & 1 & 0 & \cdots & 0 \\ -\alpha_{N-1} & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -\alpha_2 & 0 & 0 & \cdots & 1 \\ -\alpha_1 & 0 & 0 & \cdots & 0 \end{pmatrix}, \qquad C^\flat = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \end{pmatrix}$$

It is then well known that the characteristic polynomial of $A^\flat$ reads $\chi_{A^\flat}(\lambda) = \lambda^N + \alpha_N\lambda^{N-1} + \cdots + \alpha_2\lambda + \alpha_1$. Two pairs (A_1, C_1) and (A_2, C_2) in $\mathbb{Z}^{N\times N} \times \mathbb{Z}^{1\times N}$ are said to be *similar over* $\mathbb{Z}$ if there exists a matrix $T \in \mathbb{Z}^{N\times N}$ with $\det T = \pm 1$ (hence $T^{-1} \in \mathbb{Z}^{N\times N}$) such that

$$A_2 = T^{-1}A_1T, \qquad C_2 = C_1T$$

The next result provides a sufficient condition for the existence of a gain matrix L fulfilling the conditions (i′)–(ii′).

Proposition 3.1 [6]. *Let $A \in \mathbb{Z}^{N\times N}$ and $C \in \mathbb{Z}^{1\times N}$. Assume that (A, C) is similar over $\mathbb{Z}$ to a pair $(A^\flat, C^\flat)$ in a companion canonical form. Then there exists a unique matrix $L \in \mathbb{Z}^{N\times 1}$ such that the matrix $A - LC$ is Hurwitz. Furthermore, $(A - LC)^N = 0$.*

The next result shows that the information may be recovered at the receiver part.

Corollary 3.2 [6]. *Let A, C and L be as in Proposition* 3.1. *Then we may find a matrix $M \in \mathbb{Z}^{N\times 1}$ such that $(A - LC)M = 0$ and $CM = 1$. Then*

$$u_k = y_k - \hat{y}_k \quad \forall k \geqslant N \tag{3}$$

From a practical viewpoint, a pair $(A^\flat, C^\flat)$ in companion canonical form is first chosen in such a way that $A^\flat$ is invertible and it has no roots of unity as eigenvalue. Next we pick any $b \in \mathbb{T}^1$ and any matrix $T \in \mathbb{Z}^{N\times N}$ with $\det T = \pm 1$, and set $A = T^{-1}A^\flat T$ and $C = C^\flat T$. L and M are designed as in Proposition 3.1 and Corollary 3.2. Then $(\Sigma_{A,b})$ is a chaotic system, the output sequence (y_k) (which conveys the information) is equidistributed for a.e. x_0, and the information may be recovered at the receiver part after N iterations.

4. Conclusion

An encryption based on a synchronization of a chaotic motion on the N-torus has been proposed in this note. A real-time implementation has been carried out on an experimental platform involving a secured multimedia communication [9].

Acknowledgements

Lionel Rosier wishes to thank A. Bacciotti and C. Mauduit, who brought to his attention the references [5] and [8], respectively.

References

[1] C.W. Wu, L.O. Chua, A simple way to synchronize chaotic systems with applications to secure communications systems, Int. J. Bifurcation Chaos 3 (1993) 1619–1627.
[2] K.M. Cuomo, A.V. Oppenheim, S.H. Strogatz, Synchronization of Lorenz-based chaotic circuits with applications to communications, IEEE Trans. Circuits Systems II: Analog Digital Signal Process. 40 (1993) 626–633.
[3] M. Gotz, K. Kelber, W. Schwarz, Discrete-time chaotic encryption systems – part 1: statistical design approach, IEEE Trans. Circuits Systems I: Fund. Theory Appl. 44 (1997) 963–970.
[4] R.L. Devaney, An Introduction to Chaotic Dynamical Systems, 2nd ed., Addison–Wesley Publishing Company, Reading, MA, 1989.
[5] E. Vesentini, An introduction to topological dynamics in dimension 1, Rend. Sem. Mat. Univ. Politec. Torino 55 (1997) 303–357.
[6] L. Rosier, G. Millérioux, G. Bloch, Chaos synchronization for a class of discrete dynamical systems on the N-dimensional torus, in preparation.
[7] L. Kuipers, H. Niederreiter, Uniform Distribution of Sequences, John Wiley and Sons, 1974.
[8] P. Walters, An Introduction to Ergodic Theory, Springer, New York, 1975.
[9] G. Millérioux, G. Bloch, J.M. Amigo, A. Bastos, F. Anstett, Real-time video communications secured by a chaotic key stream cipher, in: Proc. of IEEE 16th European Conference on Circuits Theory and Design, ECCTD'03, Krakow, 2003, pp. 245–248.