Chaos Synchronization for a class of discrete dynamical systems on the N- dimensional torus

Lionel Rosier, Gilles Millérioux, Gérard Bloch

Chaos Synchronization for a class of discrete dynamical systems on the N-dimensional torus.

Lionel Rosier[a,*] , Gilles Millerioux[b], Gérard Bloch[b]

[a] *Universit Henri Poincar - Nancy 1, Institut Elie Cartan, BP 239, 54506 Vandœuvre-lès-Nancy Cedex, France.*

[b] *Universit Henri Poincar - Nancy 1, , Centre de Recherche en Automatique de Nancy (CRAN), ESSTIN, 2 rue Jean Lamour, 54519 Vandœuvre-lès-Nancy, France.*

Abstract

In this paper, a class of dynamical systems on the N-dimensional torus is investigated. It is proved that any dynamical system in this class is chaotic in the sense of Devaney, and that the sequences produced are equidistributed for almost every initial data. Then, the results are extended to switched affine transformations of $\mathbb{T}^N$, involving $\mathbb{Z}$-valued matrices. Next, a chaos-synchronization mechanism is introduced and used for masking information in a communication setup.

Key words: Chaotic dynamical system, switched systems, N-torus, ergodicity, chaos synchronization, cryptography.
AMS subject classifications: 34C28, 37A25, 93B55, 94A60

1 Introduction

Chaos synchronization has exhibited an increasing interest in the last decade since the pioneering works reported in [21][22]. Thereafter, it has entered the control scene and has become a very popular issue in control theory [3]. From a control theory point of view, the synchronization issue can be formulated as a state reconstruction problem. We refer the reader to [7] for a first survey of chaos synchronization techniques based on an observer approach.

Chaos synchronization has also proved to be a very common feature in physical and engineering systems, and it has been advocated as a powerful tool in secure communication [10][9][6][11][5]. Chaotic systems are indeed characterized by a great sensitivity to the initial conditions and a spreading out of the trajectories, two properties which are very close to the Shannon requirements of confusion and diffusion [15].

There are basically two approaches when using chaotic dynamical systems for secure communications purposes. The first one amounts to numerically computing a great number of iterations of a discrete chaotic system, in using e.g. the message as initial data (see [27] and the references therein). The second one amounts to hiding a message in a chaotic dynamics. Only a part of

*Corresponding author. E-mail address: rosier@iecn.u-nancy.fr

the state vector (the "output") is conveyed through the public channel. Next, a synchronization mechanism is designed to retrieve the message at the receiver part.

In both approaches, the first difficulty is to "build" a chaotic system appropriate for encryption purposes. In this context, the corresponding chaotic signals must have no patterning, a broad-band power spectrum and an auto-correlation function that quickly drops to zero. In [23], a mean for synthesizing volume-preserving or volume expanding maps is provided. For such systems, there are several directions of expansion (stretching), while the discrete trajectories are folded back into a confined region of the phase space. Expansion can be carried out by unstable linear mappings with at least one positive Lyapunov exponent. Folding can be carried out with modulo functions through shift operations, or with triangular, trigonometric functions through reflexion operations. Fully stretching piecewise affine Markov maps have also attracted interest because such maps are expanding in all directions and they have uniform invariant probability densities (see [26][8]).

Besides, we observe that the word "chaotic" has not the same meaning everywhere, and that the chaotic behavior of a system is often demonstrated only by numerical evidences. The first aim of the paper is to provide a rigorous analysis of the chaotic behavior of a large class of dynamical systems on $\mathbb{T}^N$ (the N-dimensional torus) , based on the definition given by Devaney [4]. Some connections with classical stability theory are pointed out in the paper.

For ease of design implementation and duplication, a cryptographic scheme must involve a map for which the parameters identification is expected to be a difficult task, while computational requirements for masking and unmasking information are not too heavy. The second aim of this paper is to show that all these requirements are fulfilled for a large class of affine transformations on the N-torus.

Let us now describe the content of the paper. Section 2 is devoted to the mathematical analysis of the chaotic properties of the following discrete dynamical system

$$x_{k+1} = Ax_k + b \pmod 1 \tag{1}$$

where $A \in \mathbb{Z}^{N\times N}$, $b \in \mathbb{R}^N$, and (mod 1) means that we keep the residue of $Ax_k + b$ modulo 1 (that is, the integral part of each coordinate of $Ax_k + b$ is removed). Most of the examples encountered in the literature are given only for $N = 1$ and $|A| \geq 2$, or for $N = 2$ and $\det A = 1$ (see e.g. [12]). We give here a necessary and sufficient condition for (1) to be chaotic in the sense of Devaney for any $N \geq 1$, and we investigate the equirepartition of the trajectories of (1). These results are then extended in Section 3 to the case of *switched* affine transformations of $\mathbb{T}^N$. These systems allow to generate very complicated dynamics with only a few low dimension matrices. A masking/unmasking technique based on a dynamical embedding is proposed in Section 4. The way of extracting the masked information is provided through an observer-based synchronization mechanism with a finite-time stabilization property, an issue of first importance from a practical point of view. Certain results of the paper have been announced in [25].

2 A class of chaotic dynamical systems on the N-torus

2.1 Chaotic dynamical system

Let (M, d) denote a compact metric space, and let $f : M \to M$ be a continuous map. The following definition of a chaotic system is due to Devaney [4].

Definition 1. *The discrete dynamical system*

$$(\Sigma) \qquad x_{k+1} = f(x_k)$$

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* $x_0 \in M$ *and any* $\delta > 0$*, there exists a point* $y_0 \in M$ *with* $d(x_0, y_0) < \delta$ *and an integer* $k \geq 0$ *such that* $d(x_k, y_k) \geq \varepsilon$*;*
(C2) (One-sided topological transitivity) *There exists some* $x_0 \in M$ *with* $(x_k)_{k\geq 0}$ *dense in* M*;*
(C3) (Density of periodic points) *The set* $D = \{x_0 \in M;\ \exists k > 0,\ x_k = x_0\}$ *is dense in* M*.*

Recall [30, Thm 5.9], [29, Thm 1.2.2] that when f is *onto* (i.e., $f(M) = M$), the one-sided topological transitivity is equivalent to the condition:
(C2′) For any pair of nonempty open sets U, V in M, there exists an integer $k \geq 0$ such that $f^{-k}(U) \cap V \neq \emptyset$ ($\Longleftrightarrow$ $U \cap f^k(V) \neq \emptyset$).

In this paper, we consider the case where M is the $N-$torus $\mathbb{T}^N = \mathbb{R}^N/\mathbb{Z}^N$ (quotient group). For any $X = (X_1, ..., X_N) \in \mathbb{R}^N$, the class of X in $\mathbb{T}^N$ (namely the coset $X + \mathbb{Z}^N$) is denoted by $x = \overline{X}$. Let $\pi : \mathbb{R}^N \to \mathbb{T}^N$ be the natural projection, for which $\pi(X) = x = \overline{X}$. 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 $C \in \mathbb{Z}^{P\times N}$ $(P, N \geq 1)$ and for any $X \in \mathbb{R}^N$, the class of CX in $\mathbb{T}^P$, which clearly depends only on $\overline{X}$, will be denoted by $C\overline{X}$. Thus, 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 $(\Sigma_{A,b})$ on $\mathbb{T}^N$ defined by

$$(\Sigma_{A,b}) \quad \left\{ \begin{array}{rl} x_{k+1} & = f(x_k) := Ax_k + b, \\ x_0 & \in \mathbb{T}^N. \end{array} \right. \tag{2}$$

The map f is called an *affine transformation* of the $N-$torus. When $b = 0$, f is nothing else than an endomorphism of the topological group $(\mathbb{T}^N, +)$, and f is onto (resp., an isomorphism) if and only if $\det A \neq 0$ (resp., $\det A = \pm 1$) (see [30, Thm 0.15]). Let $\mathrm{sp}(A)$ denote the spectrum of the matrix A, that is the set of the eigenvalues of A. A *root of unity* is any complex number of the form $\lambda = \exp(2\pi i t)$, with $t \in \mathbb{Q}$. To see whether a dynamical system $(\Sigma_{A,b})$ is chaotic, we need the following key result [30, Thm 1.11].

Proposition 1. *Let* $f(x) = Ax + b$ *(*$b \in \mathbb{T}^N$*,* $A \in \mathbb{Z}^{N\times N}$ *with* $\det A \neq 0$*) be an affine transformation of* $\mathbb{T}^N$*. Then the following conditions are equivalent:*

(i) $(\Sigma_{A,b})$ *is one-sided topologically transitive;*

(ii) *(a)* A *has no proper roots of unity (i.e., other than 1) as eigenvalues, and*
(b) $(A - I)\mathbb{T}^N + \mathbb{Z}b$ *is dense in* $\mathbb{T}^N$*;*

(iii) f *is* ergodic*; that is,* f *is* measure-preserving *(i.e., for any Borel set* $E \subset \mathbb{T}^N$*,* $m(f^{-1}(E)) = m(E)$*, where* m *denotes the Lebesgue measure on* $\mathbb{T}^N$*), and the only Borel sets* $E \subset \mathbb{T}^N$ *for which* $f^{-1}(E) = E$ *satisfy* $m(E) = 0$ *or* $m(E) = 1$*.*

Notice that (ii) reduces to "A has no roots of unity as eigenvalues" when $b = 0$. Indeed, it may be seen that $(A - I)\mathbb{T}^N$ is dense in $\mathbb{T}^N$ if and only if $(A - I)$ is invertible.

The first result in this paper provides a necessary and sufficient condition for $\Sigma_{A,0}$ to be chaotic.

Theorem 1. *Let* $A \in \mathbb{Z}^{N\times N}$*. Then* $(\Sigma_{A,0})$ *is chaotic if, and only if,* $\det \mathrm{A} \neq 0$ *and* A *has no roots of unity as eigenvalues.*

Proof. Assume first that $(\Sigma_{A,0})$ is chaotic. We first claim that A is nonsingular. Indeed, if $\det A = 0$, then the map f is not onto [30, Thm 0.15], i.e. $A\mathbb{T}^N \neq \mathbb{T}^N$. As $A\mathbb{T}^N$ is compact (hence equal to its closure), it is not dense in $\mathbb{T}^N$, hence we cannot find any state $x_0 \in \mathbb{T}^N$ such

that the sequence $(x_k) = (A^k x_0)$ is dense in $\mathbb{T}^N$, which contradicts (C2). Thus $\det A \neq 0$. On the other hand, since $(\Sigma_{A,0})$ is one-sided topologically transitive, the matrix A has no roots of unity as eigenvalues by virtue of Proposition 1.

Conversely, assume that $\det A \neq 0$ and that A has no roots of unity as eigenvalues. As (C1) is a consequence of (C2) and (C3) (see [2],[29, Thm 1.3.1]), we only have to establish the later properties. (C2) follows from Proposition 1. To prove (C3) we need to prove two lemmas.

Lemma 1. *Let $A \in \mathbb{Z}^{N\times N}$ be such that $\det A \neq 0$, and pick any $p \in \mathbb{N}^*$ with $(p, \det A) = 1$ (i.e. p and $\det A$ are relatively prime). Then the map $T : x \in (\mathbb{Z}/p\mathbb{Z})^N \mapsto Ax \in (\mathbb{Z}/p\mathbb{Z})^N$ is invertible.*

Proof of Lemma 1. First, observe that the map T is well-defined. Indeed, if $X, Y \in \mathbb{Z}^N$ fulfill $X - Y \in (p\mathbb{Z})^N$, then $AX - AY \in (p\mathbb{Z})^N$ so that AX and AY belong to the same coset in $(\mathbb{Z}/p\mathbb{Z})^N = \mathbb{Z}^N/(p\mathbb{Z})^N$. As $(\mathbb{Z}/p\mathbb{Z})^N$ is a finite set, we only have to prove that T is one to one. Let $X, Y \in \mathbb{Z}^N$ be such that $AX = AY$ in $(\mathbb{Z}/p\mathbb{Z})^N$ (i.e., $A(X - Y) \in (p\mathbb{Z})^N$). We aim to show that $X = Y$ in $(\mathbb{Z}/p\mathbb{Z})^N$ (i.e., $X - Y \in (p\mathbb{Z})^N$). Set $U = X - Y$, and pick a vector $Z \in \mathbb{Z}^N$ such that $AU = pZ$. It follows that $U = \frac{p}{\det A}\tilde{A}Z$, where $\tilde{A} \in \mathbb{Z}^{N\times N}$ denotes the adjoint matrix of A (i.e. the transpose of the matrix formed by the cofactors). Since $U \in \mathbb{Z}^N$, each component of the vector $p\tilde{A}Z$ is divisible by $\det A$. Since $(p, \det A) = 1$, we infer the existence of a vector $V \in \mathbb{Z}^N$ such that $\tilde{A}Z = (\det A)V$. Then $X - Y = U = pV \in (p\mathbb{Z})^N$, as desired. ■

Lemma 2. *Let A and p be as in Lemma 1, and let $E_p := \{\overline{0}, \overline{(\frac{1}{p})}, ..., \overline{(\frac{p-1}{p})}\} \subset \mathbb{T}$. Then each point $x \in E_p^N$ is periodic for $(\Sigma_{A,0})$. As a consequence, the set of periodic points of $(\Sigma_{A,0})$ is dense in $\mathbb{T}^N$ (i.e., (C3) is satisfied).*

Proof of Lemma 2. First, observe that for any $i, j \in \{0, ..., p-1\}$, $i/p \equiv j/p \pmod 1$ if and only if $i \equiv j \pmod p$. We infer from Lemma 1 that the map $\tilde{T} : x \in E_p^N \mapsto Ax \in E_p^N$ is well defined and invertible. Pick any $x \in E_p^N$. As the sequence $(\tilde{T}^k x)_{k\geq 1}$ takes its values in the (finite) set E_p^N, there exist two numbers $k_2 > k_1 \geq 1$ such that $\tilde{T}^{k_1}x = \tilde{T}^{k_2}x$. $\tilde{T}$ being invertible, we conclude that $A^{k_2-k_1}x = x$ (i.e., x is a periodic point). Finally, the set $E = \cup\{E_p;\ p \geq 1,\ (p, \det A) = 1\}$ is clearly dense in $\mathbb{T}^N$ (take for p any large prime number), and all its points are periodic. This completes the proof of Lemma 2 and of Theorem 1. ■

For an affine transformation, we obtain a very similar result to Theorem 1 when $1 \notin \mathrm{sp}(A)$.

Corollary 1. *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.*

Proof. Pick any $B \in \mathbb{R}^N$ with $\overline{B} = b$. As $1 \notin \mathrm{sp}(A)$, we may perform the change of variables

$$x = r - \overline{(A - I)^{-1}B}, \tag{3}$$

which transforms (2) into

$$\left\{ \begin{array}{rl} r_{k+1} & = Ar_k, \\ r_0 & = x_0 + \overline{(A - I)^{-1}B}. \end{array} \right. \tag{4}$$

Clearly, the conditions (C2) and (C3) are fulfilled for $(\Sigma_{A,b})$ if and only if they are fulfilled for (4). Therefore, the result is a direct consequence of Theorem 1. ■

2.2 Equidistribution

Let us consider now a discrete dynamical system with an output

$$\left\{ \begin{array}{rl} x_{k+1} & = Ax_k + b \\ y_k & = Cx_k \end{array} \right.$$

where $x_0 \in \mathbb{T}^N$, $A \in \mathbb{Z}^{N\times N}$, $b \in \mathbb{T}^N$ and $C \in \mathbb{Z}^{1\times N}$. It should be expected that the output y_k inherits the chaotic behavior of the state x_k. However, Devaney's definition of a chaotic system cannot be tested on the sequence (y_k), since this sequence is not defined as a trajectory of a dynamical system. Rather, we may give a condition ensuring that the sequence (y_k) is equidistributed (hence dense) in $\mathbb{T}$ for a.e. x_0, a property which may be seen as an *ersatz* of (C2).

If $X = (X_1, ..., X_N), Y = (Y_1, ..., Y_N)$ are any given points in $[0,1)^N$ and $x = \overline{X}$, $y = \overline{Y}$, then we say that $x < y$ (resp., $x \leq y$) if $X_i < Y_i$ (resp., $X_i \leq Y_i$) for $i = 1, ..., N$. The set of points $z \in \mathbb{T}^N$ such that $x \leq z < y$ will be denoted by $[x, y)$. Let $(x_k)_{k\geq 0}$ be any sequence in $\mathbb{T}^N$. For any subset E of $\mathbb{T}^N$, let $S_K(E)$ denote the number of points x_k, $0 \leq k \leq K-1$, which lie in E.

Definition 2. *[13] We say that* (x_k) *is* uniformly distributed modulo 1 *(or* equidistributed in $\mathbb{T}^N$*) if*

$$\lim_{K\to\infty} \frac{S_K([x,y))}{K} = m([x,y)) = \prod_{i=1}^{N}(Y_i - X_i)$$

for all intervals $[x, y) \subset \mathbb{T}^N$.

The following result is very useful to decide whether a sequence is equidistributed or not.

Proposition 2. *(***Weyl criterion** *[13], [24]) The sequence* $(x_k)_{k\geq 0}$ *is equidistributed in* $\mathbb{T}^N$ *if, and only if, for every lattice point* $p \in \mathbb{Z}^N$, $p \neq 0$

$$\frac{1}{K}\sum_{0\leq k<K} e^{2i\pi p\cdot x_k} \to 0 \qquad \text{as } K \to +\infty.$$

The next result shows that under the same assumptions as in Corollary 1 the sequences (x_k) and (y_k) are respectively equidistributed in $\mathbb{T}^N$ and $\mathbb{T}$ for a.e. initial state $x_0 \in \mathbb{T}^N$.

Theorem 2. *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 (2)) is equidistributed in* $\mathbb{T}^N$*, and the sequence* $(y_k) = (Cx_k)$ *is equidistributed in* $\mathbb{T}$.

Proof: By virtue of Theorem 1, the map $f(x) = Ax + b$ is ergodic on $\mathbb{T}^N$. It follows then from Birkhoff Ergodic Theorem (see e.g. [30, Thm 1.14]) that for any $h \in L^1(\mathbb{T}^N, dm)$ and for a.e. $x_0 \in \mathbb{T}^N$

$$\frac{1}{K}\sum_{0\leq k<K} h(f^k(x_0)) \to \int_{\mathbb{T}^N} h(y)\, dm(y) \qquad \text{as } K \to +\infty.$$

Therefore, for every lattice point $p \in \mathbb{Z}^N$, $p \neq 0$, and for a.e. $x_0 \in \mathbb{T}^N$

$$\frac{1}{K}\sum_{0\leq k<K} e^{2\pi ip\cdot f^k(x_0)} \to \int_{\mathbb{T}^N} e^{2\pi ip\cdot y}\, dm(y) = 0 \qquad \text{as } K \to +\infty.$$

As $\mathbb{Z}^N \setminus \{0\}$ is countable, the same property holds for a.e. $x_0 \in \mathbb{T}^N$ and all $p \in \mathbb{Z}^N \setminus \{0\}$. Therefore, we infer from Weyl criterion that the sequence $(x_k) = (f^k(x_0))$ is equidistributed for a.e. $x_0 \in \mathbb{T}^N$. Pick any $x_0 \in \mathbb{T}^N$ such that (x_k) is equidistributed, and let us show that the output sequence $(y_k) = (Cx_k)$ is also equidistributed provided that $C = (C_1, ..., C_N) \neq (0, ..., 0)$. Indeed, for any $p \in \mathbb{Z} \setminus \{0\}$

$$\frac{1}{K}\sum_{0\leq k<K} e^{2\pi ipy_k} = \frac{1}{K}\sum_{0\leq k<K} e^{2\pi i(pC)\,x_k} \to 0 \qquad \text{as } K \to +\infty,$$

hence the equidistribution of (y_k) follows again by Weyl criterion. ■

2.3 Links between stability and chaoticity

It has been demonstrated in Theorem 1 that a system $\Sigma_{A,0}$ is chaotic if and only if the spectrum of A does not contain 0 nor a root of unity. The proof of this result was based upon ergodicity theory. The aim of this section is to provide a direct proof of this result (more precisely, of (C_2')) in the more familiar situation where A is a "dilating matrix", i.e.

$$\mathrm{sp}(A) \subset \{z \in \mathbb{C};\ |z| > 1\}. \tag{5}$$

In stability words, the condition (5) amounts to saying that the linear system $X_{k+1} = A^{-1}X_k$ is asymptotically stable in $\mathbb{C}^N$. The following result is obtained in using classical stability arguments.

Lemma 3. *Let $A \in \mathbb{Z}^{N\times N}$ fulfilling (5), and let U be any nonempty open set in $\mathbb{T}^N$. Then there exists a number $k \in \mathbb{N}^*$ such that $f^k(U) = \mathbb{T}^N$, where $f(x) = Ax$.*

Proof. We claim that we are done if we show that for any $X \in \mathbb{R}^N$ and any (arbitrary small) $\varepsilon > 0$, we may pick a $k > 0$ such that

$$A^k X + [0,1)^N \subset A^k\, B_\varepsilon(X). \tag{6}$$

($B_\varepsilon(X)$ denoting the open ball in $\mathbb{R}^N$ centered at X with radius ε). Indeed, we infer from (6) that

$$\mathbb{T}^N = \pi(A^k X + [0,1)^N) \subset \pi(A^k\, B_\varepsilon(X)) = f^k(\pi(B_\varepsilon(X)))$$

and the result of the lemma follows at once. It remains to show that (6) holds true. As $\mathrm{sp}(A^{-1}) \subset \{z \in \mathbb{C};\ |z| < 1\}$, the linear system $X_{k+1} = A^{-1}X_k$ is asymptotically stable in $\mathbb{C}^N$, hence there exists a $k > 0$ such that $A^{-k}[0,1)^N \subset B_\varepsilon(0)$. Therefore, $[0,1)^N \subset A^k B_\varepsilon(0)$, and $A^k X + [0,1)^N \subset A^k(X + B_\varepsilon(0)) = A^k B_\varepsilon(X)$, as desired. ∎

It follows from Lemma 3 that if (5) holds true, then the system $(\Sigma_{A,0})$ is one-sided topologically transitive (as $(C2')$ is clearly satisfied).

3 Chaotic switched systems

In this section we extend the results of Section 2 to switched affine systems on the $N-$dimensional torus.

3.1 Switched systems

To define what we mean by a switched system, we assume given a sequence $(A_j)_{1\le j\le J}$ of matrices in $\mathbb{Z}^{N\times N}$ and a sequence $(b_j)_{1\le j\le J}$ of points in $\mathbb{T}^N$, and we consider the following (periodic) switching signal $\sigma : \mathbb{N} \to \{1, ..., J\}$ defined as

$$\sigma(k + pJ) = k + 1 \quad \forall k \in \{0, ..., J-1\},\ \forall p \in \mathbb{N}. \tag{7}$$

Notice that $\sigma(k + J) = \sigma(k)$ for all $k \ge 0$.

Definition 3. *The switched system $\Sigma_{A,b,\sigma}$ associated with the sequences $A = (A_j)_{1\le j\le J}$, $b = (b_j)_{1\le j\le J}$ and the switching signal σ is defined by*

$$(\Sigma_{A,b,\sigma}) \qquad x_{k+1} = A_{\sigma(k)}x_k + b_{\sigma(k)} \quad \forall k \ge 0. \tag{8}$$

If e.g. $J = 2$ and $b_1 = b_2 = 0$, then the first terms of the sequence (x_k) read $x_1 = A_1 x_0$, $x_2 = A_2 x_1 = A_2 A_1 x_0$, $x_3 = A_1 x_2 = A_1 A_2 A_1 x_0$, etc. Notice that (8) defines a dynamical system associated with a *particular* switching signal. Having in mind the applications to chaos synchronization and cryptography, we shall not consider (as in [1]) the case where the switching signal is any random function $\sigma : \mathbb{N} \to \{1, ..., J\}$.

The first issue of interest is the chaotic behavior of (8). A direct inspection of Devaney's definition cannot be made, since the dynamical system (8) is *time-varying*. However, using the periodic structure of the switching signal, we shall see in the next section that it is possible to put the dynamical system (8) into a time invariant form.

3.2 Time-invariant form

We first perform a change of variables as in the proof of Corollary 1, namely

$$r_k = x_k + z_{\sigma(k)} \qquad \forall k \geq 0 \tag{9}$$

where the points $z_j \in \mathbb{T}^N$ for $j = 1, ..., J$ are chosen in such a way that

$$r_{k+1} = A_{\sigma(k)} r_k \qquad \forall k \geq 0. \tag{10}$$

Straightforward calculations show that (10) is satisfied provided that

$$z_{\sigma(k+1)} = A_{\sigma(k)} z_{\sigma(k)} - b_{\sigma(k)} \qquad \forall k \in \{0, ..., J-1\},$$

i.e.

$$\begin{cases} z_2 &= A_1 z_1 - b_1, \\ z_3 &= A_2 z_2 - b_2, \\ &\vdots \\ z_J &= A_{J-1} z_{J-1} - b_{J-1}, \\ z_1 &= A_J z_J - b_J. \end{cases} \tag{11}$$

The resolution of (11) is then reduced to the resolution of the following single equation

$$(A_J A_{J-1} \cdots A_1 - I) z_1 = A_J \cdots A_2 b_1 + \cdots + A_J b_{J-1} + b_J. \tag{12}$$

When $1 \notin \mathrm{sp}(A_J A_{J-1} \cdots A_1)$, then writing $b_j = \overline{B_j}$ for each j and setting

$$Z_1 := (A_J A_{J-1} \cdots A_1 - I)^{-1} (A_J \cdots A_2 B_1 + \cdots + A_j B_{J-1} + B_J),$$

we obtain that $z_1 := \overline{Z_1}$ is a solution to (12). Defining z_2, ...,z_J by (11), we conclude that for this choice of $z_1, ..., z_J$, the change of variables (9) transforms (8) into (10).

Let $\mathcal{Z} := (z_1, ..., z_J)$, $G := \{(x_0, A_1 x_0, A_2 A_1 x_0, ..., A_{J-1} \cdots A_1 x_0);\ x_0 \in \mathbb{T}^N\}$, and $M := G - \mathcal{Z}$. Consider the map $\phi : \mathbb{T}^N \to G$, defined by $\phi(x_0) = (x_0, A_1 x_0, ..., A_{J-1} \cdots A_1 x_0)$. Then G is a compact connected subgroup of $(\mathbb{T}^N)^J$ (hence a Lie group), and ϕ is a group isomorphism which is continuous together with its inverse. It follows that the map $h : x_0 \in \mathbb{T}^N \mapsto \phi(x_0) - \mathcal{Z} \in M$ is also continuous together with its inverse. Thus $M = \{h(x_0);\ x_0 \in \mathbb{T}^N\}$ may as well be considered as the state space. A simple computation shows that for any $p \geq 0$

$$\begin{cases} r_{pJ} &= (A_J \cdots A_1)^p r_0 \\ r_{pJ+1} &= A_1 r_{pJ} = (A_1 A_J \cdots A_2)^p A_1 r_0 \\ &\vdots \\ r_{pJ+J-1} &= (A_{J-1} \cdots A_1 A_J)^p A_{J-1} \cdots A_1 r_0, \end{cases}$$

that is

$$\mathcal{R}_{p+1} = \mathcal{A}^p \mathcal{R}_0 \tag{13}$$

with $\mathcal{R}_p = (r_{pJ}, r_{pJ+1}, \ldots, r_{pJ+J-1})^T \in G$ and

$$\mathcal{A} = \begin{pmatrix} A_J \cdots A_1 & 0 & \cdots & \cdots \\ 0 & A_1 A_J A_{J-1} \cdots A_2 & 0 & \cdots \\ \cdots & 0 & \ddots & 0 \\ \cdots & \cdots & 0 & A_{J-1} \cdots A_1 A_J \end{pmatrix} \in \mathbb{Z}^{NJ \times NJ}. \tag{14}$$

(13) may be rewritten as

$$\mathcal{R}_{p+1} = \mathcal{A}\mathcal{R}_p, \quad \forall p \geq 0. \tag{15}$$

Letting $\mathcal{X}_p = (x_{pJ}, x_{pJ+1}, \ldots, x_{pJ+J-1})^T \in M$ (hence $\mathcal{X}_p = \mathcal{R}_p - \mathcal{Z}$), we have that $\mathcal{X}_{p+1} = \mathcal{A}\mathcal{X}_p + (\mathcal{A} - I)\mathcal{Z}$. The above considerations may be summarized in the following result.

Proposition 3. *Assume that 1 is not an eigenvalue of the matrix $A_J A_{J-1} \cdots A_1$. Then the switched system (8) may be seen as the following time-invariant dynamical system in M:*

$$\mathcal{X}_{p+1} = \mathcal{A}\mathcal{X}_p + (\mathcal{A} - I)\mathcal{Z} \qquad \forall p \geq 0. \tag{16}$$

3.3 Chaoticity and equidistribution

(16) may be seen as the restriction to M of a time invariant linear dynamical system on $\mathbb{T}^{NJ}$ to which the theory developed in Section 2 may be applied. The first result of this section provides a sufficient condition for (16) to be chaotic.

Theorem 3. *Assume that the matrix $\mathcal{A}$ in (14) is invertible and has no root of unity as eigenvalues. Then the dynamical system (15) is chaotic on G, and the dynamical system (16) is chaotic on M.*

Proof. As the map $\mathcal{R} \in G \mapsto \mathcal{X} \in M$ is an isometry, it is sufficient to prove that (15) is chaotic on G. To keep the same notations as above, we consider (16) with $\mathcal{Z} = 0$ (hence $M = G$). We infer from Theorem 1 that (16) is chaotic on $\mathbb{T}^{NJ}$ (not G !). To prove that the restriction of (16) to G is still chaotic, we check that the conditions in Definition 1 are fulfilled. First of all, it is easily seen that the map $\mathcal{X}_0 \mapsto \mathcal{A}\mathcal{X}_0$ from G into itself is onto. Next, as the map $X \mapsto \mathcal{A}X$ is one-sided topologically transitive (and ergodic) by virtue of Theorem 1, we infer that there exists a state $X = (x_0, ..., x_{J-1}) \in (\mathbb{T}^N)^J$ such that the sequence $(\mathcal{A}^k X)_{k \geq 0}$ is dense in $\mathbb{T}^{NJ}$. It follows that the sequence of the N first components $((A_J \cdots A_1)^k x_0)_{k \geq 0}$ is dense in $\mathbb{T}^N$. Since ϕ is a homeomorphism from $\mathbb{T}^N$ onto G, and $\phi((A_J \cdots A_1)^k x_0) = \mathcal{A}^k \mathcal{X}_0$ with $\mathcal{X}_0 = \phi(x_0)$, we conclude that the sequence $(\mathcal{A}^k \mathcal{X}_0)_{k \geq 0}$ is dense in G, i.e. (C_2) is fulfilled. As (C_1) follows from (C_2) and (C_3), it remains to check that (C_3) holds true. By Lemma 2, each point of the form $(x_0, A_1 x_0, ..., A_{J-1} \cdots A_1 x_0)$ with $x_0 \in E_p^N$ is periodic for (16) provided that $(p, \det A) = 1$. As the set $\{(x_0, A_1 x_0, ..., A_{J-1} \cdots A_1 x_0);\ x_0 \in E_p^N,\ p \geq 1,\ (p, \det \mathcal{A}) = 1\}$ is dense in G, we conclude that (C_3) is satisfied. Therefore, (16) is a chaotic system on M. ■

Remark 1. *The restriction of a chaotic system to a stable subgroup may fail to be chaotic, as is shown by the following example. Consider the dynamical system $(\Sigma_{A,0})$ in $\mathbb{T}^2$ with $A = \begin{pmatrix} -3 & 1 \\ -1 & 0 \end{pmatrix}$. Then $(\Sigma_{A,0})$ is chaotic on $\mathbb{T}^2$, as the spectrum of A is $\sigma(A) = \{\frac{-3 \pm \sqrt{5}}{2}\}$. Let G denote the projection on $\mathbb{T}^2$ of the eigenspace associated with the eigenvalue $\frac{-3+\sqrt{5}}{2}$, i.e. $G = \pi(Ker(A - \frac{-3+\sqrt{5}}{2} I))$. Clearly, (C_1) fails to be true for $(\Sigma_{A,0})$ restricted to G, for $|\frac{-3+\sqrt{5}}{2}| < 1$.*

An equidistribution property follows under the same assumptions.

Corollary 2. *Let $\mathcal{A}$ be as in Theorem 3, and let $C \in \mathbb{Z}^{1\times N} \setminus \{0\}$. Then for a.e. $x_0 \in \mathbb{R}^N$ the sequence (x_k) (defined in (8)) is equidistributed in $\mathbb{T}^N$, and the sequence $(y_k) = (Cx_k)$ is equidistributed in $\mathbb{T}$.*

Proof. Assume first that $\mathcal{Z} = 0$, (i.e. $b_1 = \cdots = b_J = 0$). It follows from [30, Thm 1.11 p. 31] that the map $\mathcal{X}_0 \mapsto \mathcal{A}\mathcal{X}_0$ is ergodic on G, hence for any $h \in L^1(G, d\mu)$ and for a.e. $\mathcal{X}_0 \in G$

$$\frac{1}{K}\sum_{0\le k<K} h(\mathcal{A}^k\mathcal{X}_0) \to \int_G h(\mathcal{X})d\mu(\mathcal{X}) \qquad \text{as } K \to +\infty,$$

where μ denotes the Haar measure on G (see e.g. [30]). It is easy to check that $\mu(\phi(B)) = m(B)$ for any Borel set $B \subset \mathbb{T}^N$. Therefore

$$\int_G h(\mathcal{X})\, d\mu(\mathcal{X}) = \int_{\mathbb{T}^N} h(\phi(x))\, dm(x).$$

Pick $h(x_0, x_1, ..., x_{J-1}) = e^{2\pi i(p_0x_0+\cdots+p_{J-1}x_{J-1})}$ with $(p_0, ..., p_{J-1}) \in (\mathbb{Z}^N)^J \setminus \{0\}$. Taking $p_0 \neq 0$ and $p_1 = \cdots = p_{J-1} = 0$, there obtains

$$\frac{1}{K}\sum_{0\le k<K} e^{2\pi i p_0\cdot x_{kJ}} \to \int_{\mathbb{T}^N} e^{2\pi i p_0\cdot x}\, dm(x) = 0,$$

hence the sequence $(x_{kJ})_{k\ge 0}$ is equidistributed. A similar argument shows that the subsequences (x_{kJ+1}), ..., (x_{kJ+J-1}) are equidistributed as well. It follows that the sequence (x_k) is equidistributed in $\mathbb{T}^N$. When $\mathcal{Z} \neq 0$, the above argument shows that the sequences (r_{kJ}), (r_{kJ+1}),...,(r_{kJ+J-1}) are equidistributed. Using the periodicity of σ, we conclude that the sequences (x_{kJ}), (x_{kJ+1}),..., (x_{kJ+J-1}) are equidistributed, hence (x_k) is equidistributed in $\mathbb{T}^N$. The proof that the sequence (y_k) is equidistributed in $\mathbb{T}$ is as above. ■

4 Synchronization and information recovering

The aim of this section is to suggest a chaos-based encryption scheme involving affine transformations on the $N-$torus. It differs from the one introduced in [18] in the fact that the maps involve $\mathbb{Z}$-valued matrices. New stability results are provided in this framework. To be precise, we provide some conditions which guarantee a synchronization with a *finite* transient time despite the inherent nonlinearity of the chaotic systems under study.

4.1 Encryption setup

At each discrete time k, a symbol $m_k \in \mathbb{T}$ (the *plaintext*) of a sequence $(m_k)_{k\ge 0}$ is encrypted by a (nonlinear) encrypting function e which "mixes" m_k and x_k and produces a *ciphertext* $u_k = e(x_k, m_k)$. We also assume given a decrypting function d such that $m_k = d(x_k, u_k)$ for each k. Next, the ciphertext u_k is embedded in the dynamics exhibited by the map (8). We shall consider the following encryption

$$(\Sigma_{A,b,M,C,\sigma}) \qquad \left\{ \begin{array}{rl} x_{k+1} & = A_{\sigma(k)}(x_k + M_{\sigma(k)}u_k) + b_{\sigma(k)} \\ y_k & = C_{\sigma(k)}(x_k + M_{\sigma(k)}u_k) \end{array} \right. \tag{17}$$

which corresponds to an embedding of the ciphertext in both the dynamics and the output. In (17) $A_{\sigma(k)} \in \mathbb{Z}^{N\times N}$, $M_{\sigma(k)} \in \mathbb{Z}^{N\times N}$, $C_{\sigma(k)} \in \mathbb{Z}^{N\times 1}$ are matrices belonging to the respective families

$(A_j)_{1\le j\le J}$, $(M_j)_{1\le j\le J}$, and $(C_j)_{1\le j\le J}$, and $b_{\sigma(k)} \in \mathbb{T}^N$ is a vector belonging to the family $(b_j)_{1\le j\le J}$. σ is the switching signal as defined in (7). $y_k \in \mathbb{T}$ is the output conveyed to the receiver through the channel.

From the definition of the decrypting function d, it is clear that to retrieve m_k at the decryption side we need to recover the pair (x_k, u_k), which in turn calls for reproducing a chaotic sequence $(\hat{x}_k)$ synchronized with (x_k) (i.e., such that $\hat{x}_k - x_k \to 0$). To this end, we propose a mechanism based on some suitable switched unknown input observers, inspired from the ones given in [18] and [19]. The main differences are that: (i) the gain matrices have to be $\mathbb{Z}$-valued because of the congruential operations; (ii) a finite-time synchronization is achieved for obvious practical reasons.

For the encryption considered here, the decryption involves the following observer-like structure

$$(\hat{\Sigma}_{A,b,M,C,\sigma}) \qquad \left\{ \begin{array}{rl} \hat{x}_{k+1} & = A_{\sigma(k)}\hat{x}_k + L_{\sigma(k)}(y_k - \hat{y}_k) + b_{\sigma(k)} \\ \hat{y}_k & = C_{\sigma(k)}\hat{x}_k \end{array} \right. \tag{18}$$

where $\hat{x}_k \in \mathbb{T}^N$ and $\hat{y}_k \in \mathbb{T}$ ($\hat{x}_0$ being an arbitrary point in $\mathbb{T}^N$). We stress that $\hat{x}_{k+1}$ and $\hat{y}_k$ are well defined provided that the observer gain $L_{\sigma(k)}$ is $\mathbb{Z}-$valued.

Setting $e_k = x_k - \hat{x}_k$, when subtracting (18) from (17) we obtain that the error dynamics reads

$$e_{k+1} = (A_{\sigma(k)} - L_{\sigma(k)}C_{\sigma(k)})e_k + (A_{\sigma(k)} - L_{\sigma(k)}C_{\sigma(k)})M_{\sigma(k)}u_k \tag{19}$$

Before proceeding to the design of the observers, we give a few definitions and a preliminary result.

4.2 Definitions and preliminary results

Definition 4. *A pair $(A^\flat, C^\flat)$ is said to be in a* companion canonical form *if it takes the form*

$$A^\flat = \begin{pmatrix} -\alpha^{N-1} & 1 & 0 & \cdots & 0 \\ -\alpha^{N-2} & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -\alpha^{1} & 0 & 0 & \cdots & 1 \\ -\alpha^{0} & 0 & 0 & \cdots & 0 \end{pmatrix}, \qquad C^\flat = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \end{pmatrix}. \tag{20}$$

It is well known that the characteristic polynomial of $A^\flat$ reads $\chi_{A^\flat}(\lambda) = \lambda^N + \alpha^{N-1}\lambda^{N-1} + \cdots + \alpha^1\lambda + \alpha^0$.

Definition 5. *Two pairs (A, C) and $(A^\flat, C^\flat)$ 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 $T^{-1} \in \mathbb{Z}^{N\times N}$ too) such that*

$$A = T^{-1}A^\flat T, \quad C = C^\flat T.$$

The following result provides a sufficient condition for an observable pair (A, C) to admit a $\mathbb{Z}$-valued gain matrix L such that $A - LC$ is Hurwitz.

Proposition 4. *Let $A \in \mathbb{Z}^{N\times N}$ and $C \in \mathbb{Z}^{1\times N}$ be two time-invariant matrices. Assume that (A, C) is similar over $\mathbb{Z}$ to a pair $(A^\flat, C^\flat)$ in a companion canonical form (the first column of $A^\flat$ reads $(-\alpha^{N-1} \ \ldots \ -\alpha^0)'$). Then there exists a unique matrix $L \in \mathbb{Z}^{N\times 1}$ such that the matrix $A - LC$ is Hurwitz (i.e., $sp(A - LC) \subset \{z \in \mathbb{C};\ |z| < 1\}$), namely $L = T^{-1}L^\flat$ with $L^\flat = (-\alpha^{N-1} \ \ldots \ -\alpha^0)'$. Furthermore, $(A - LC)^N = 0$.*

Proof. Write $A = T^{-1}A^\flat T$, $C = C^\flat T$, with $(A^\flat, C^\flat)$ as in (20) and $T \in \mathbb{Z}^{N\times N}$ with $\det T = \pm 1$. For any given matrix $L \in \mathbb{Z}^{N\times 1}$, we define the matrix $L^\flat = (l^{N-1} \cdots \ l^0)'$ by $L^\flat = TL$. Then, $A - LC = T^{-1}(A^\flat - L^\flat C^\flat)T$ with

$$A^\flat - L^\flat C^\flat = \begin{pmatrix} -\alpha^{N-1} - l^{N-1} & 1 & 0 & \cdots & 0 \\ -\alpha^{N-2} - l^{N-2} & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -\alpha^1 - l^1 & 0 & 0 & \cdots & 1 \\ -\alpha^0 - l^0 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Its characteristic polynomial reads

$$\chi_{A^\flat - L^\flat C^\flat}(\lambda) = \lambda^N + (\alpha^{N-1} + l^{N-1})\lambda^{N-1} + \cdots + (\alpha^1 + l^1)\lambda + (\alpha^0 + l^0).$$

If L is such that $A - LC$ is Hurwitz, then $A^\flat - L^\flat C^\flat = T(A - LC)T^{-1}$ is Hurwitz too, hence we may write $\chi_{A-LC}(\lambda) = \chi_{A^\flat - L^\flat C^\flat}(\lambda) = \lambda^p \chi(\lambda)$, where $p \in \{0, ..., N\}$ and $\chi \in \mathbb{Z}[\lambda]$ has its roots $\lambda_1, ..., \lambda_{N-p}$ in the set $\{z \in \mathbb{C};\ 0 < |z| < 1\}$. Assume that $p < N$, and denote by q the constant coefficient of χ. Then $q \neq 0$ (since $\chi(0) \neq 0$), and $|q| = \prod_{i=1}^{N-p} |\lambda_i| < 1$, which is impossible, since $q \in \mathbb{Z}$. Therefore $p = N$ and $l^j = -\alpha^j$ for any $j \in \{0, ..., N-1\}$ (hence $L^\flat$ and L are unique). On the other hand

$$A^\flat - L^\flat C^\flat = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}. \tag{21}$$

For this choice of L, $\chi_{A-LC}(\lambda) = \lambda^N$ and $(A - LC)^N = 0$. ∎

It should be emphasized that the above argument shows that a $\mathbb{Z}$-valued matrix $\mathcal{N}$ is Hurwitz if and only if it is nilpotent. In other words, the system $\nu_{k+1} = \mathcal{N}\nu_k$ is *asymptotically stable* if and only if it is *finite-time stable*.

4.3 Synchronization of switched systems

Consider a switched system

$$\nu_{k+1} = \mathcal{N}_{\sigma(k)}\nu_k \tag{22}$$

in which each matrix in $(\mathcal{N}_j)_{1\leq j\leq N}$ is nilpotent. The following result proves to be useful to guarantee that the state vector ν_k reaches zero in finite time.

Lemma 4. *Let $\mathcal{N}_1, ..., \mathcal{N}_N$ be N nilpotent matrices in $\mathbb{C}^{N\times N}$. Assume that the Lie algebra spanned by these matrices is resoluble. Then $\mathcal{N}_1\mathcal{N}_2 \cdots \mathcal{N}_N = 0$.*

Proof. Let $\mathrm{Lie}(\mathcal{N}_1, ..., \mathcal{N}_N)$ denote the Lie algebra spanned by the matrices $\mathcal{N}_1, ..., \mathcal{N}_N$. Since $\mathrm{Lie}(\mathcal{N}_1, ..., \mathcal{N}_N)$ is resoluble, we infer from Lie theorem (see e.g. [28, Theorem 3.7.3]) that there exists an invertible matrix $T \in \mathbb{C}^{N\times N}$ such that each matrix $\mathcal{N}_j' := T^{-1}\mathcal{N}_j T$ is upper triangular with zeros on the diagonal. Now, a straightforward computation shows that $\mathcal{N}_1' \cdots \mathcal{N}_N' = 0$. ∎

Remark 2. *The Lie algebraic condition in Lemma 4 is useful, since the product of N nilpotent matrices in $\mathbb{C}^{N\times N}$ may fail to be nilpotent without any additional assumption. Indeed, we observe that* $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. *It is however easy to see that the product of N nilpotent matrices which commute pairwise is 0. Lemma 4 provides a nice generalization of this observation.*

The following result is the main result of this section.

Theorem 4. *Let us consider (17) and (18). Assume that the following conditions are fulfilled for each $j = 1, \ldots, J$:*

1) *the pair (A_j, C_j) is similar over $\mathbb{Z}$ to a pair $(A_j^\flat, C^\flat)$ in a companion canonical form through $T_j \in \mathbb{Z}^{N\times N}$ with* $\det T_j = \pm 1$*;*

2) *the matrix T_j may be written in the form $T_j = S_j T$ with S_j being upper triangular of determinant ± 1, T being any square matrix in $\mathbb{Z}^{N\times N}$ with $\det T = \pm 1$;*

3) *the matrix $M_j \in \mathbb{Z}^{N\times 1}$ is such that $M_j = T_j^{-1} M^\flat$ with*

$$M^\flat \;=\; (1\ 0\ \ldots\ 0)'; \tag{23}$$

4) *the matrix $L_j \in \mathbb{Z}^{N\times 1}$ is such that $L_j = T_j^{-1} L_j^\flat$ with*

$$L_j^\flat \;=\; \big(-\alpha_j^{N-1} \ldots\ -\alpha_j^0\big)'. \tag{24}$$

Then the error (19) fulfills $e_k = 0$ for $k \geq N$ and for any $\hat{x}_0$ in (18). Furthermore, $\hat{u}_k := y_k - C_{\sigma(k)}\hat{x}_k = u_k$ for $k \geq N$.

Proof. On one hand, if 1) and 4) are fulfilled, a simple computation leads to

$$A_j - L_j C_j = T_j^{-1}(A_j^\flat - L_j^\flat C^\flat) T_j = T_j^{-1} \mathcal{N} T_j \tag{25}$$

with

$$\mathcal{N} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

$\mathcal{N}$ is clearly a nilpotent, upper triangular matrix. Moreover, from 1) and 3), $(A_j - L_j C_j) M_j = T_j^{-1} \mathcal{N} M_j^\flat$ and $\mathcal{N} M_j^\flat = 0$. As a result, $(A_j - L_j C_j) M_j = 0$, hence

$$e_{k+1} = \big(A_{\sigma(k)} - L_{\sigma(k)} C_{\sigma(k)}\big) e_k, \ \forall k \geq 0. \tag{26}$$

Iterated applications of (26) yield

$$e_{j+pJ} = (A_j - L_j C_j) \cdots (A_1 - L_1 C_1) \{(A_J - L_J C_J) \cdots (A_1 - L_1 C_1)\}^p e_0. \tag{27}$$

with, from 1) and 2), $A_j - L_j C_j = T^{-1}(S_j^{-1} \mathcal{N} S_j) T$. Let now $\mathcal{T}$ denote the set of upper triangular complex matrices. It is well-known that $\mathcal{T}$ is a resoluble Lie algebra (see [28, p. 201]). As each matrix $S_j^{-1} \mathcal{N} S_j$ is upper triangular, the Lie algebra $\mathrm{Lie}(S_1^{-1}\mathcal{N}S_1, S_2^{-1}\mathcal{N}S_2, ..., S_J^{-1}\mathcal{N}S_J)$ is a Lie subalgebra of $\mathcal{T}$, hence it is resoluble. The same property holds true for

$$\mathrm{Lie}(A_1 - L_1 C_1, ..., A_J - L_J C_J) = T^{-1} \mathrm{Lie}(S_1^{-1}\mathcal{N}S_1, S_2^{-1}\mathcal{N}S_2, ..., S_J^{-1}\mathcal{N}S_J) T.$$

It follows then from Lemma 4 that $e_k = 0$ for all $k \geq N$.

On the other hand, according to (17),

$$y_k = C_{\sigma(k)}(x_k + M_{\sigma(k)} u_k) = C_{\sigma(k)} e_k + C_{\sigma(k)} \hat{x}_k + C_{\sigma(k)} M_{\sigma(k)} u_k$$

hence, as $C_{\sigma(k)} M_{\sigma(k)} = 1$,

$$\hat{u}_k := y_k - C_{\sigma(k)} \hat{x}_k = C_{\sigma(k)} e_k + u_k = u_k \quad \forall k \geq N.$$

■

Remark 3. *1. The choice $S_j = I$ for all j in 2) corresponds to the case when the matrices T_j are identical and equal to T.*

2. The result in Theorem 4 is sharp for $N = 2$. Indeed, let $T_1, T_2 \in \mathbb{Z}^{2\times 2}$ be any matrices with determinant ± 1, and let $\mathcal{N} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. Then a direct computation shows that the matrix $(T_2^{-1}\mathcal{N}T_2)(T_1^{-1}\mathcal{N}T_1)$ is nilpotent if and only if $Lie(S_2^{-1}\mathcal{N}S_2, \mathcal{N})$ is resoluble (where $S_2 = T_2T_1^{-1}$), if and only if S_2 is upper triangular.

4.4 Concluding remarks

The *message-embedding* masking technique studied here does not originate from the conventional cryptography (see [16] for a good survey). Nevertheless, it seems to be highly related to some popular encryption schemes, the so-called *stream ciphers* [20]. Therefore, it is desirable that the proposed scheme be robust against both statistical and algebraic attacks. On one hand, the robustness against statistical attacks follows from the chaotic behavior of the output. On the other hand, the security against algebraic attacks mainly rests on the identification of the parameters of the system which is a hard task here for two reasons:

1. The particular *structure* of the encryption system ($\Sigma_{A,b,M,C,\sigma}$), that is the *dimension* and the *number* of the matrices A_j, is assumed to be unknown;

2. The ciphertext u_k actually results from a mixing between the plaintext m_k and the state x_k ($u_k = e(x_k, m_k)$). This generally results in a *nonlinear* dynamics ($\Sigma_{A,b,M,C,\sigma}$), rendering the parameters hardly identifiable [14].

A real-time implementation has already been carried out on an experimental platform involving a secured multimedia communication. (For details about the platform, see e.g. [17]). The security aspects are currently investigated and are out of the scope of the paper.

Acknowledgments. One of the authors (L.R.) wishes to thank A. Bacciotti and C. Mauduit, who brought to his attention the references [29] and [30], respectively.

References

[1] A. Agrachev and D. Liberzon. Lie-algebraic stability criteria for switched systems. *SIAM J. Control Optim.*, 40(1):253–269 (electronic), 2001.

[2] J. Banks, J. Brooks, G. Cairns, G. Davis, and P. Stacey. On Devaney's definition of chaos. *Amer. Math. Monthly*, 99(4):332–334, 1992.

[3] V. D. Blondel, E. D. Sontag, M. Vidyasagar, and J. C. Willems. *Open Problems in Mathematical Systems and Control Theory.* Communication and Control Engineering. Springer Verlag, 1999.

[4] R. Devaney. *An introduction to chaotic dynamical systems.* Studies in Nonlinearity. Westview Press, Boulder, CO, 2003. Reprint of the second (1989) edition.

[5] I.I. Blekhman E. Mosekilde, A.L. Fradkov, editor. *Special Issue on Chaos Synchronization and Control*, volume 58. elsevier, 2002.

[6] Kolumban G., Kennedy M. P., and Chua L. O. The role of synchronization in digital communications using chaos - part I: Fundamentals of digital communications. *IEEE Trans. Circuits. Syst. I (Special issue on Chaos Synchronization and Control:Theory and applications)*, 44:927–936, October 1998.

[7] Nijmeijer H. and Mareels I. M. Y. An observer looks at synchronization. *IEEE Trans. Circuits. Syst. I: Fundamental Theo. Appl*, 44:882–890, October 1997.

[8] M. Hasler, M. Delgado-Restituto, and A. Rodriguez-Vasquez. Markov maps for communications with chaos. In *Proc. of the 1996's Nonlinear Dynamics in Electronic Systems, NDES'96*, pages 161–166, Sevilla, June 1996.

[9] Special Issue. Chaos synchronization and control : theory and applications. *IEEE Trans. Circuits. Syst. I: Fundamental Theo. Appl*, 44(10):853–1039, 1997.

[10] Special Issue. Control of chaos and synchronization. *Syst. Control Letters*, 31:259–322, 1997.

[11] Special Issue. Control and synchronization of chaos. *International Journal of Bifurcation and Chaos*, 10(4), 2000.

[12] A. Katok and B. Hasselblatt. *Introduction to the modern theory of dynamical systems*, volume 54 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1995. With a supplementary chapter by Katok and Leonardo Mendoza.

[13] L. Kuipers and H. Niederreiter. *Uniform distribution of sequences*. Wiley-Interscience [John Wiley & Sons], New York, 1974. Pure and Applied Mathematics.

[14] L. Ljung and T. Glad. On global identifiability for arbitrary model parametrizations. *Automatica*, 30:265–276, 1994.

[15] J.L. Massey. *Contemporary cryptology: an introduction*. in : G.J. Simmons (Ed.), Contemporary Cryptology, IEEE Press, New York, 1992.

[16] A. J. Menezes, P. C. Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, October 1996.

[17] G. Millerioux, G. Bloch, J. M. Amigo, A. Bastos, and F. Anstett. Real-time video communication secured by a chaotic key stream cipher. In *Proc. of IEEE 16th European Conference on Circuits Theory and Design, ECCTD'03*, pages 245–248, Krakow, Poland, September 1-4 2003.

[18] G. Millerioux and J. Daafouz. An observer-based approach for input independent global chaos synchronization of discrete-time switched systems. *IEEE Trans. Circuits. Syst. I: Fundamental Theo. Appl*, 50(10):1270–1279, 2003.

[19] G. Millerioux and J. Daafouz. Input independent chaos synchronization of switched systems. *IEEE Trans. on Automatic Control*, 49(7):1182 – 1187, July 2004.

[20] G. Millérioux, A. Hernandez, and JM Amigo. Conventional cryptography and message-embedding. In *Proc. of International Symposium on Nonlinear Theory and its Applications, NOLTA'2005*, Bruges, October 2005.

[21] L.M. Pecora and T.L. Carroll. Synchronization in chaotic systems. *Phys. Rev. Lett.*, 64:821–824, 1990.

[22] L.M. Pecora and T.L. Carroll. Driving systems with chaotic signals. *Phys. Rev. A*, 44(8):2374–2383, August 1991.

[23] L.M. Pecora, T.L. Carroll, G. Johnson, and D. Mar. Volume-preserving and volume-expanding synchronized chaotic systems. *Physical review E*, 56(5):5090 – 5100, November 1997.

[24] G. Rauzy. *Propriétés statistiques de suites arithmétiques*. Presses Universitaires de France, Paris, 1976. Le Mathématicien, No. 15, Collection SUP.

[25] L. Rosier, G. Millérioux, and G. Bloch. Chaos synchronization on the $n-$torus and cryptography. *Comptes Rendus Mécanique*, 332(12):969–972, 2004.

[26] R. Rovatti and G. Setti. On the distribution of synchronization times in coupled uniform piecewise-linear markov maps. *IEICE Transactions on Fundamentals*, 81(9):1769–1776, 1998.

[27] R. Schmitz. Use of chaotic dynamical systems in cryptography. *Journal of the Franklin Institute*, 338:429–441, 2001.

[28] V. S. Varadarajan. *Lie groups, Lie algebras, and their representations*, volume 102 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1984. Reprint of the 1974 edition.

[29] E. Vesentini. An introduction to topological dynamics in dimension one. *Rend. Sem. Mat. Univ. Politec. Torino*, 55(4):303–357 (1999), 1997. Jacobian conjecture and dynamical systems (Torino, 1997).

[30] P. Walters. *An introduction to ergodic theory*, volume 79 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1982.