Flat Dynamical Systems and Self-Synchronizing Stream Ciphers

Gilles Millérioux, Philippe Guillot, Jose Maria Amigo, Jamal Daafouz

FLAT DYNAMICAL SYSTEMS AND SELF-SYNCHRONIZING STREAM CIPHERS

G. Millérioux[1], P. Guillot[2], J. M. Amigó[3] and J. Daafouz[4]

Abstract. In this paper, we present properties of dynamical systems and their use for cryptographical applications. In particular, we study the relationship with the self-synchronizing stream ciphers from a structural point of view. Finally a framework involving discrete Lyapunov exponents and Walsh transform is sketched to characterize the dynamical behaviors.

1. Introduction

The main objective of the paper is to show how dynamical systems can be used for cryptographical applications, in particular for the design of self-synchronizing stream ciphers. The reasoning is based on structural characterization of dynamical systems which confer to them special synchronization properties. And yet, synchronization issues are of special importance. Indeed, in a stream cipher cryptographic setup, the correspondents generate the same key stream to hide the message and this requires perfect synchronization. The advantage of self-synchronizing stream cipher lies in that the receiver automatically recovers the synchronization only from the cipher text. These ciphers have been studied, for example, in [6]. Recall also that block ciphers can be operated in a self-synchronizing (so-called CFB) mode.

[1] Nancy Université, Centre de Recherche en Automatique de Nancy, France email: gilles.millerioux@esstin.uhp-nancy.fr
[2] Université Paris 8, France, email: philippe.guillot@univ-paris8.fr
[3] University of Elche, Alicante, Spain, email: jm.amigo@umh.es
[4] Nancy Université, Centre de Recherche en Automatique de Nancy, France email: jamal.daafouz@ensem.inpl-nancy.fr

J-F. Michon, P. Valarcher, J-B. Yunès (Eds.): BFCA'08

The paper is organized as follows. In Sect. 2, three important notions related to dynamical systems borrowed from control theory are presented: relative degree, invertibility and flatness. In Sect. 3, a connection is established between ciphers defined by *flat* dynamical systems and self-synchronizing stream ciphers. In Sect. 4, two examples of construction of self-synchronizing stream ciphers based on flat dynamical systems are provided. Finally, in Sect.5 and Sect.6, a framework involving discrete Lyapunov exponents and Walsh transform is provided to characterize the dynamical behaviors of the proposed ciphers.

2. Dynamical systems

2.1. Basic definition

The dynamical systems considered here are discrete-time ones. Their behavior depends on the internal state and the input values. They produce an output signal. A formal definition is given below.

Definition 2.1. A dynamical system is a 5-tuple $\mathcal{D} = (A, B, S, f, h)$ where

(1) A is the input alphabet, which is a finite set of input symbols denoted a_t at the discrete time t;
(2) B is the output alphabet, which is a finite set of output symbols denoted b_t at the discrete time t;
(3) S is the finite set of internal states denoted s_t at the discrete time t;
(4) $f : S \times A \longrightarrow S$ is the next-state function. Given an input $a_t \in A$ and a state $s_t \in S$, the state vector a time $t + 1$ reads:

$$s_{t+1} = f(s_t, a_t) \tag{1}$$

(5) $h : S \times A \longrightarrow B$ is the output function. Given an input $a_t \in A$ and a state $s_t \in S$, the output symbol reads:

$$b_t = h(s_t, a_t) \tag{2}$$

The sequence (b_t) produced by the dynamical system $\mathcal{D}$ is completely defined by the initial internal state s_0 and by the input sequence (a_t) of symbols a_t.

The internal state $s_{t+i} \in S$ at time $t + i$ depends on the state $s_t \in S$ and on the sequence of i input symbols $a_t \cdots a_{t+i-1} \in A^i$, by means of

the so called i-order iterated next-state function, $f^{(i)} : S \times A^i \longrightarrow S$, defined for $i \geq 1$ and recursively obeying for $t \geq 0$

$$\begin{cases} f^{(1)}(s_t, a_t) = f(s_t, a_t) \\ f^{(i+1)}(s_t, a_t \cdots a_{t+i}) = f(f^{(i)}(s_t, a_t \cdots a_{t+i-1}), a_{t+i}) \text{ for } i \geq 1 \end{cases}$$

Similarly, the output symbol b_{t+i} at time $t+i$ depends on the state $s_t \in S$ and on the sequence of $i+1$ input symbols $a_t \cdots a_{t+i} \in A^{i+1}$, by means of the so-called i-order iterated output function $h^{(i)} : S \times A^{i+1} \longrightarrow B$, defined for $i \geq 0$ and recursively obeying for $t \geq 0$

$$\begin{cases} h^{(0)}(s_t, a_t) = h(s_t, a_t) \\ h^{(i)}(s_t, a_t \ldots a_{t+i}) = h(f^{(i)}(s_t, a_t \cdots a_{t+i-1}), a_{t+i}) \text{ for } i \geq 1, \end{cases}$$

When such a system corresponds to a physical process model, all the variables, namely the input, the output and the state belong to a continuum. When the variables belong to finite cardinality sets, the dynamical systems reduce to finite-state automata which are also known as Mealy or Moore machines. The next subsections are devoted to the presentation of three important properties related to those systems and borrowed from the automatic control theory: relative degree, left invertibility and flatness. It will be shown in Sect. 3 that considering the three above-mentioned properties is of special interest for cryptographic purposes. Indeed, for ciphering applications, such dynamical systems may be used to transform a plaintext a into a cryptogram b. The secret element that parameterizes the encryption process may be either the next-state function or the output function, or any combination of those two parameters. For the decryption, a device achieving the inversion is required.

2.2. **Relative degree**

Definition 2.2. The relative degree of the dynamical system $\mathcal{D}$ is the quantity equalling

- 0 if $\exists s_t \in S,\ \exists a_t, a'_t \in A \quad h(s_t, a_t) \neq h(s_t, a'_t)$
- r if for any sequence $a_{t+i} \cdots a_{t+r}$ $(i > 0)$ of input symbols

$$\exists s_t \in S,\ \exists a_t, a'_t \in A \quad h^{(r)}(s_t, a_t a_{t+1} \cdots a_{t+r}) \neq h^{(r)}(s_t, a'_t a'_{t+1} \cdots a'_{t+r})$$

In other words, the relative degree of the dynamical system $\mathcal{D}$ is the minimum number of iterations such that the output at time $t + r$ is influenced by the input at time t and

- if the relative degree r of $\mathcal{D}$ equals zero, there exists a state $s_t \in S$ and two distinct input symbols $a_t \in A$ and $a'_t \in A$ that lead to different values of the output
- if the relative degree is $r > 0$, then for $i < r$, the iterated output function $h^{(i)}$ only depends on s_t while for $i \geq r$, it depends both on s_t and on the sequence of $i - r + 1$ input symbols $a_t \cdots a_{t+i-r}$. In particular, for $i = r$, the iterated output function depends both on a_t and on s_t, that is, there exists a state $s_t \in S$ and two distinct input symbols $a_t \in A$ and $a'_t \in A$ that lead to different values of the output, for any sequence $a_{t+i} \cdots a_{t+r}$ of input symbols.

Consequently, for $r > 0$, the r-order output function $h^{(r)}$ may be considered as a function over $S \times A$ and thereby one has for $r \geq 0$:

$$b_{t+r} = h^{(r)}(s_t, a_t) \tag{3}$$

Remark 1. *We do not consider the case when r may depend on a. Hereafter, the relative degree will be an intrinsic parameter of* $\mathcal{D}$

As a result, if a dynamical system $\mathcal{D} = (A, B, S, f, h)$ has a relative degree equal to r, then the dynamical system $\mathcal{D}' = (A, B, S, f, h^{(r)})$ is equivalent to $\mathcal{D}$ in the sense that it has the same behavior as $\mathcal{D}$ provided that the first r output symbols are ignored. The block diagram of $\mathcal{D}$ is depicted on Figure 1.

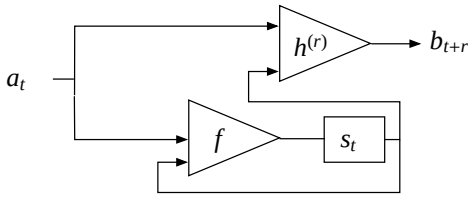

FIGURE 1. Block diagram of $\mathcal{D}$

In the cryptographic context, the advantage of a relative degree $r > 0$ lies in that it can be expected that the cryptographic complexity of the cipher increases while the computational complexity does not since $h^{(r)}$ results from recursive operations.

2.3. **Left invertibility**

The invertibility property is obviously required in cryptography. For a given encryption dynamical system $\mathcal{D}_E$, there must exist a decryption

one $\mathcal{D}_D$ that recovers efficiently the plaintext from the cryptogram. Let us mention that it is not mandatory to recover all the plain text. It may be acceptable to recover the plain text only after a finite number of synchronization symbols. More precisely, if a dynamical system is used for ciphering, then the receiver must be able to recover the plain text a from the cipher text b. From the dynamical system theory, it implies the so-called left invertibility.

Definition 2.3. The dynamical system $\mathcal{D}$ is *left invertible* if there exists a nonnegative integer $R < \infty$, called *inherent delay*, such that for any two inputs $a_t \in A$ and $a'_t \in A$ the following implication holds:

$$\begin{aligned} &\forall s_t \in S \\ &h^{(0)}(s_t, a_t) \cdots h^{(R)}(s_t, a_t \cdots a_{t+R}) = h^{(0)}(s_t, a'_t) \cdots h^{(R)}(s_t, a'_t \cdots a'_{t+R}) \\ &\Rightarrow a_t = a'_t \end{aligned} \tag{4}$$

The left invertibility property means that the input a_t is uniquely determined by the knowledge of the state s_t and of the output sequence $b_t, \ldots, b_{t+R}$.

When left invertible, $\mathcal{D}$ admits an inverse dynamical system $\mathcal{D}^{-1}$ which is generically defined as the 5−tuple $\mathcal{D}^{-1} = (B, A, S_R, f', h')$ where

(1) B is the input alphabet of $\mathcal{D}^{-1}$, which is the output alphabet of $\mathcal{D}$;
(2) A is the output alphabet of $\mathcal{D}^{-1}$, which is the input alphabet of $\mathcal{D}$;
(3) $S_R = S \times B^R$ is the finite set of internal states, constituted of both the internal state $s_t \in S$ and the required input sequence $b_t, \ldots, b_{t+R-1}$ to determine symbol a_t.
(4) $f' : S_R \times B \longrightarrow S_R$ is the inverse next-state function. Given an output sequence $b \in B^{R+1}$ and $s'_t \in S$, the state obeys the following dynamics:

$$(s'_{t+R+1}, b_{t+1} \cdots b_{t+R}) = f'(s'_{t+R}, b_t \cdots b_{t+R-1}, b_{t+R})$$

By construction of the inverse next-function, the internal states s_t of the transmitter and the S−component s'_t of the internal state of the receiver fulfill $s'_{t+t_0+R} = s_{t+t_0}$ for all $t \geq 0$ if $s'_{t_0+R} = s_{t_0}$.
(5) $h' : S_R \times B \longrightarrow A$ is the inverse output function. Given an output sequence $b \in B^{R+1}$ and $s'_t \in S$ one has:

$$h'(s'_{t+R}, b_t \cdots b_{t+R-1}, b_{t+R}) = a'_{t+R} = a_t \text{ if } s'_{t+R} = s_t$$

In other words, the inversion is correctly performed with a delay R provided that the sequences (s_t) and (s'_t) are synchronized at both ends.

Remark 2. *Hereafter it will be assumed that the inherent delay and the relative degree coincide, that is $R = r$. The class of dynamical systems for which such an assumption holds can be easily characterized.*

We assume now that the input alphabet A equals the output alphabet B, and that the information is included in a substring of the input sequence. If so, the invertibility property means that for any internal state $s_t \in S$, the map

$$h_{s_t} : \begin{array}{ccc} A & \longrightarrow & A \\ a_t & \longmapsto & h^{(r)}(s_t, a_t) \end{array}$$

is a permutation, where $r \geq 0$ is the relative degree of $\mathcal{D}$. The output function $h^{(r)}$ may be considered as a family of permutations, indexed by the set S of the internal states, or at least by a subset.

In the binary case, one has $A = B = \{0, 1\}$. The only permutations are identity and inversion. Thus the output function $h^{(r)}$ may be always expressed as $h^{(r)}(s_t, a_t) = a_t \oplus h_1(s_t)$, where h_1 is a map $S \longrightarrow \{0, 1\}$ and where $\oplus$ denotes the modulo 2 addition on the 2-element field. Let us mention that in the general (non-binary) case, the output function $h^{(r)}$ is expressed as $h^{(r)}(s_t, a_t) = \sigma_{h_1(s_t)}(a_t)$, where $(\sigma_p)_{p \in P}$ is a family of permutations on A indexed by a subset P of S.

2.4. **Flatness**

Definition 2.4. An output for $\mathcal{D}$ is said to be *flat* if all system variables of $\mathcal{D}$ can be expressed as a function of b_t and a finite number of its forward/backward iterates. In particular, there exists a function $\mathcal{F}$ and integers $t_1 < t_2$ such that

$$s_t = \mathcal{F}(b_{t+t_1}, \cdots, b_{t+t_2}) \tag{5}$$

Definition 2.5. The dynamical system $\mathcal{D}$ is said to be *flat* if it admits a flat output.

We define the *flatness characteristic number* as the quantity $d = t_2 - t_1 + 1$.

A necessary condition for flatness is left invertibility. If the system is flat, then there exist at least two ways for obtaining the function $\mathcal{F}$ and so the relation (5): direct and recursive. The first solution is based on the elimination of the state s_t in equations (1) and (3). A second solution consists in resorting to the next-state iterated inverse function defined for $i \geq 1$ by $f'^{(i)} : S_R \times B^i \longrightarrow S'$ recursively obeying for $t \geq 0$

$$\begin{cases} f'^{(1)}(s'_{t+R}, b_t \cdots b_{t+R-1}, b_{t+R}) = f'(s'_{t+R}, b_t \cdots b_{t+R-1}, b_{t+R}) \\ f'^{(i+1)}(s'_{t+R}, b_t \cdots b_{t+R-1}, b_{t+R} \cdots b_{t+R+i}) \\ = f'(f'^{(i)}(s'_{t+R}, b_t \cdots b_{t+R-1}, b_{t+R} \cdots b_{t+R+i-1}), b_{t+R+i}) \end{cases}$$

By construction of the iterated inverse next-function, the internal states s_t of the transmitter and the $S-$component s'_t of the internal state of the receiver fulfill $s'_{t+i+R+1} = f'^{(i+1)}(s'_{t+R}, b_t \cdots b_{t+R-1}, b_{t+R} \cdots b_{t+R+i}) = s_{t+i+1}$ for all $t \geq 0$ if $s'_{t+R} = s_t$.

Assume that there exists an integer I such that $f'^{(I+1)}$ does no longer depend on the state s'_{t+R}. Hence, the following equalities apply

$$\begin{aligned} & f'^{(I+1)}(s'_{t+R}, b_t \cdots b_{t+R-1}, b_{t+R} \cdots b_{t+R+I}) \\ &= f'^{(I+1)}(s_t, b_t \cdots b_{t+R-1}, b_{t+R} \cdots b_{t+R+I}) \\ &= s_{t+I+1} \\ &= f'^{(I+1)}(0, b_t \cdots b_{t+R-1}, b_{t+R} \cdots b_{t+R+I}) \end{aligned}$$

is always fulfilled. Hence,

$$s_t = f'^{(I+1)}(0, b_{t-I-1} \cdots b_{t+R-1}). \tag{6}$$

Equation (6) gives explicitly the function $\mathcal{F} = f'^{(I+1)}$, the bounds $t_1 = -I - 1$, $t_2 = R - 1$ and the flatness characteristic number $d = R + I + 1$. The existence of I is guaranteed if the system $\mathcal{D}$ is flat.

3. The connection with self-synchronizing stream ciphers

Assume that the dynamical system $\mathcal{D}$ has bounded relative degree r and that it is flat with a flatness characteristic number d. If so, the following claims apply:

- there exists a function $h^{(r)}$, such that $b_{t+r} = h^{(r)}(s_t, a_t)$ depends both on s_t and a_t

- the state s_t of $\mathcal{D}$ can always be expressed as a function of the output and this function reads $s_t = \mathcal{F}(b_{t+t_1}, \cdots, b_{t+t_2})$. The flatness property expresses the fact that the receiver may synchronize his internal state automatically, without any other information but the cipher text. This corresponds exactly to the so-called self-synchronizing stream cipher. The synchronization delay of the cipher is $d = t_2 - t_1 + 1$

As a result, if these conditions are fulfilled, the dynamical system $\mathcal{D}$ acts as a self-synchronizing stream cipher with the canonical representation given on Figure 2. Since the principle is based upon the embedding of the input a into the dynamics f, it will be called Self-synchronizing Message-Embedded Stream Cipher.

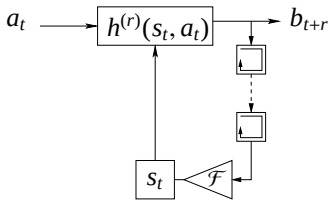

FIGURE 2. Self-synchronizing Message-Embedded Stream Cipher

The inverse of a flat dynamical system $\mathcal{D}$ can always be expressed as a canonical form defined by

(1) The internal state set S is the set of $d-$tuple of output symbols : $S = B^d = \{(b_{t-1}, \cdots, b_{t-d}) \mid b_{t-i} \in B\}$.
(2) The next-state inverse function is a shift $f'(b_t, (b_{t-1}, \ldots, b_{t-d})) = (b_t, b_{t-1}, \ldots, b_{t-d+1})$.
(3) The output function is any function $h : A \times S \longrightarrow B$ such that $h(b_t, b_{t-1}, \ldots b_{t-d}) = \sigma_{g(b_{t-1},\ldots b_{t-d})}(b_t)$, where $g(b_{t-1}, \ldots b_{t-d})$ is a function that selects a permutation $\sigma_i : A \longrightarrow B$.

The security of such a canonical self-synchronizing stream cipher is insured as long as the permutation $\sigma_{g(b_{t-1},\ldots b_{t-d})}$ defined from the internal state cannot be distinguished from a random choice in the set of all permutations.

In practice, the actual synchronization delay of self-synchronizing stream ciphers is the number of symbols required for the receiver to recover the same internal state as the transmitter. It is usual to define a statistical synchronization delay as a random variable D_s that is a delay

of synchronization regarding the input sequence (b_t) and the receiver internal state s'_t as random variables. A self-synchronizing stream cipher is said to have statistical synchronization delay if the probability that $D_s > D_0$ decreases as D_0 grows to infinity. And yet, as previously pointed out, the synchronization delay of the proposed cipher obtained from $\mathcal{D}$ is $d = t_2 - t_1 + 1$. As a result, for designing a self-synchronizing stream cipher with statistical synchronization delay, the quantities t_1 and/or t_2 must depend on (b_t) and s'_t. Regarding cryptographic applications, it may be expected to bring in more complex dynamic.

4. Self-synchronizing message-embedded stream cipher construction

In this section, an example of construction of self-synchronizing stream cipher based on flat dynamical systems involving picewise linear nonlinearities is provided. The flatness condition is expressed in terms of algebraic conditions (see [7] for details). Let $\mathbb{F}$ be a finite field. All along this section, the input and output alphabets are $A = \mathbb{F}$ and $B = \mathbb{F}$. The internal state is the n dimensional vector space over $\mathbb{F}$.

We first address the design with linear dynamical systems although any cryptographic application makes senses when resorting to this class of systems. The following subsection is only viewed as a prerequisite.

4.1. Flat linear system

A dynamical system is linear if the next-state and the output functions are linear. A linear dynamical system denoted $\mathcal{D}_L$ can be generically described by:

$$\begin{cases} s_{t+1} = f(s_t, a_t) &= Ms_t + va_t \\ b_t = h(s_t, a_t) &= Cs_t + Da_t \end{cases} \tag{7}$$

where $M \in \mathbb{F}^{n\times n}$, $v \in \mathbb{F}^{n\times 1}$, $C \in \mathbb{F}^{1\times n}$ and $D \in \mathbb{F}$.

In general, the relative degree r of $\mathcal{D}_L$ coincides with the inherent delay R. It equals zero if $D \neq 0$. If $D = 0$, then the relative degree is the minimum number $r > 0$ such that $CA^{r-1}B \neq 0$. It can be shown that the next-state iterated inverse function of $\mathcal{D}_L$ is defined for $i \geq 1$ by

$f'^{(i)} : S' \times B^{i+1} \longrightarrow S'$ recursively obeying for $t \geq 0$

$$\begin{cases} f'^{(1)}(s'_{t+R}, b_{t+R}) = Ps'_{t+R} + Qb_{t+R} \\ f'^{(i+1)}(s'_{t+R}, b_{t+R} \cdots b_{t+R+i}) = P^{i+1}s'_{t+R} + Q^{i+1}b_{t+R} \\ \quad +Q^i b_{t+R+1} + \cdots + Qb_{t+R+i} \end{cases}$$

where P and Q are some matrices depending on M, v, C and D.

Such a system $\mathcal{D}_L$ is flat with flat output b_t if and only if there exists an integer I such that the matrix P^{I+1} is the null matrix, so that $f'^{(I+1)}$ does no longer depend on s'_{t+R}. In other words, the matrix P defining the next-state inverse function must be nilpotent.

4.2. **Flat switched linear systems**

Switched linear systems denoted $\mathcal{D}_s$ are of the form

$$\begin{cases} f(s_t, a_t) = s_{t+1} &= M_{\sigma(t)}s_t + v_{\sigma(t)}a_t \\ h(s_t, a_t) = b_t &= C_{\sigma(t)}s_t + D_{\sigma(t)}a_t \end{cases} \tag{8}$$

All the matrices, namely $M_{\sigma(s)} \in \mathbb{F}^{n\times n}$, $v_{\sigma(s)} \in \mathbb{F}^{n\times 1}$, $C_{\sigma(s)} \in \mathbb{F}^{1\times n}$ and $D_{\sigma(s)} \in \mathbb{F}$ belong to the respective finite sets of matrices $\{M_j\}_{1\leq j\leq J}$, $\{v_j\}_{1\leq j\leq J}$, $\{C_j\}_{1\leq j\leq J}$ and $\{D_j\}_{1\leq j\leq J}$. The index j corresponds to the discrete mode of the system and results from a switching function $\sigma : t \mapsto j = \sigma(t) \in \{1, \ldots, J\}$.

It can be shown that the relative degree r of $\mathcal{D}_s$ coincides with the inherent delay R. The relative degree r of $\mathcal{D}_s$ is

- $r = 0$ if for all modes j, $D_{\sigma(t)} \neq 0$;
- the least integer $r < \infty$ such that, for all $t \geq 0$

$$\begin{array}{l} \mathcal{T}^{i,j}_{\sigma(t)} = 0 \text{ for } i = 0, \ldots, r-1 \text{ and } j = 0, \ldots, i \\ \mathcal{T}^{r,0}_{\sigma(t)} \neq 0 \end{array} \tag{9}$$

with

$$\mathcal{T}^{i,j}_{\sigma(t)} = C_{\sigma(t+i)}M^{\sigma(t+i-1)}_{\sigma(t+j+1)}v_{\sigma(t+j)} \text{ if } j \leq i-1,\ \mathcal{T}^{i,i}_{\sigma(t)} = D_{\sigma(t+i)} \tag{10}$$

and with the transition matrix defined as the product of matrices

$$\begin{array}{rcl} M^{\sigma(t_1)}_{\sigma(t_0)} &=& M_{\sigma(t_1)}M_{\sigma(t_1-1)} \ldots M_{\sigma(t_0)} \text{ if } t_1 \geq t_0 \\ &=& \mathbf{1}_n \text{ if } t_1 < t_0 \end{array}$$

where $\mathbf{1}_n$ stands for the identity matrix of dimension n.

It can be shown that the next-state iterated inverse function of $\mathcal{D}_s$ is defined for $i \geq 1$ by $f'^{(i)} : S' \times B^{i+1} \longrightarrow S'$ recursively obeying for $t \geq 0$

$$\begin{cases} f'^{(1)}(s'_{t+R}, b_{t+R}) = P_{\sigma(t)} s'_{t+R} + Q_{\sigma(t)} b_{t+R} \\ f'^{(i+1)}(s'_{t+R}, b_{t+R} \cdots b_{t+R+i}) = P_{\sigma(t+i)} \cdots P_{\sigma(t)} s'_{t+R} + \\ P_{\sigma(t+i)} \cdots P_{\sigma(t+1)} Q_{\sigma(t)} b_{t+R} + \\ \quad P_{\sigma(t+i)} \cdots P_{\sigma(t+2)} Q_{\sigma(t+1)} b_{t+R+1} + \cdots + P_{\sigma(t+i)} Q_{\sigma(t+i-1)} b_{t+R+i-1} \\ \quad + Q_{\sigma(t+i)} b_{t+R+i} \end{cases}$$

where P_j and Q_j are some matrices depending on M_j, v_j, C_j and D_j. Let $\mathcal{P}$ and $\mathcal{Q}$ be the sets of those possible matrices.

Such a system $\mathcal{D}_s$ is flat with flat output b_t if and only if there exists an integer I such that the matrix $P_{\sigma(t+I)} \cdots P_{\sigma(t)}$ is the null matrix, so that $f'^{(I+1)}$ does no longer depend on s'_{t+R}. Therefore, the following proposition applies:

Proposition 4.1. *The system $\mathcal{D}_L$ is a self-synchronizing stream cipher if the two following conditions are satisfied:*

(1) *The product $P_{j_1} \cdots P_{j_I}$ of any I matrices belonging to the set $\mathcal{P}$ equals the null matrix.*
(2) *The switching function σ is self-synchronizing, that is, it must only depend on a subsequence of (b_t).*

The synchronization delay is bounded by I. When the probability that the product of I factors $P_{j_1} \cdots P_{j_I}$ equals the zero matrix grows to 1 as I grows to infinity, then the synchronization delay is statistically bounded.

The construction of a self-synchronizing switching function can follow the scheme of the canonical flat dynamical systems. The construction of flay dynamical systems can be extended to dynamical systems with non-linear transitions.

5. Discrete chaos and cryptography

We have seen in Sect. 2.3 that when, as usual, the input alphabet A and the output alphabet B are the same, the output functions $h^{(r)}_{s_t} : a_t \mapsto h^{(r)}(s_t, a_t)$ are a family of permutations of A, parameterized by the internal states s_t. Permutations, together with substitutions,

are the basic tools in block encryption. One of the techniques used to design permutations (and pseudo-random sequences) for cryptographical applications is the discretization of chaotic maps (see e.g. [4]). Let X be a compact metrical space (like an n-dimensional interval or an n-torus) and $f : X \to X$ a map. Roughly speaking, we say that the dynamical system (X, f) generated by the iterates $f^n = f \circ f^{n-1}$ ($f^0 =$ identity) is chaotic if the the orbits $\{f^n(x) : n \in \mathbb{N}\}$ have random-like properties for 'typical' choices of $x \in X$ (see [8] for a formal definition of chaos). Chaos-based cryptography takes advantage of the ergodic properties of dynamical systems.

The intuition that permutations may have different diffusion and mixing properties have been embodied in an approach called discrete chaos, whose theoretical framework was presented in [5]. The main tool of discrete chaos is the discrete Lyapunov exponent.

Let $\mathcal{X} = \{\xi_0, ..., \xi_{L-1}\}$ be a linearly ordered finite set, $\xi_i < \xi_{i+1}$, endowed with a metric $d(\cdot, \cdot)$, and $F : \mathcal{X} \to \mathcal{X}$ be a bijection or, equivalently, a permutation of $\mathcal{X}$. We define the *discrete Lyapunov exponent* (DLE) of F as

$$\lambda_F = \frac{1}{L} \sum_{i=0}^{L-1} \log \frac{d\left(F(\xi_{i+1}), F(\xi_i)\right)}{d\left(\xi_{i+1}, \xi_i\right)}, \tag{11}$$

where the definition of ξ_L, the right neighbor of ξ_{L-1}, depends on the 'topology' of $\mathcal{X}$ (see below for a choice). We will use natural logarithms to calculate λ_F. Observe that λ_F depends both on the order (that determines whose neighbor is who) and on the metric d, but it is invariant under rescaling and, furthermore, has the same invariances that d might have.

Any discrete approximation of a chaotic system (X, f) in form of a permutation $F_M : \{0, 1, ..., M-1\} \to \{0, 1, ..., M-1\}$ is called a chaotic cryptographic primitive. Furthermore, we say that a cryptographic algorithm is chaotic if some of its building blocks is a chaotic cryptographic primitive. Examples of chaotic primitives include the finite-state tent map, the finite-state Chebyshev map and the finite-state n-dimensional torus automorphisms. Affine transformations on the n-torus in chaos synchronization-based cryptography have been studied in [10]. These maps have the nice property that the precision of the initial point does not degrade along its orbit. See [2] for a general view of digital chaotic

cryptography.

In the examples and applications we will consider below, F will be a permutation of the subset $\mathcal{X} = \{0, ..., L-1\}$ of $\mathbb{R}$ endowed with the Euclidean distance $d(\xi_i, \xi_j) = \left|\xi_i - \xi_j\right|$ and the standard order. In this case, we will refer to $\mathcal{X}$ as a linear set and choose $\xi_L \equiv \xi_{L-2}$ to be the 'right' neighbor of the last (or greatest) state ξ_{L-1} in the definition (11); we have $\lambda_F \geq 0$.

The justification for calling λ_F the discrete Lyapunov exponent of F is as follows. Let $x_{j+1} = f(x_j)$, $j = 0, 1, ..., L-1$, be a typical trajectory of length L of a chaotic self-map f of a one-dimensional interval I, such that $x_{j+1} \neq x_j$ for all j and $|x_{L-1} - x_0| < \varepsilon$. We define $f(x_{L-1}) = x_0$ and order $x_0, x_1, ..., x_{L-1}$ in I to obtain $x_{n_0} < x_{n_1} < ... < x_{n_{L-1}}$, so that x_{n_i} and $x_{n_{i+1}}$ are neighbors. Furthermore, set $\xi_i = \lfloor x_{n_i} N \rfloor$, where N is chosen such that $\xi_i \neq \xi_j$ for all $i \neq j$. The map f induces then the obvious permutation

$$F(\xi_i) = \xi_j \text{ if } f(x_{n_i}) = x_{n_j}$$

on $\{\xi_0, ..., \xi_{L-1}\}$. Then,

Proposition 5.1. *[5] Let I be a one-dimensional interval and $f : I \to I$ a chaotic map with piecewise continuous derivative. Then $\lim_{L\to\infty} \lambda_{F_L} = \lambda_f$, where λ_f is the Lyapunov exponent of f.*

In [5] the reader can also find a generalization of Proposition 5.1 to higher dimensions.

We consider next some examples of permutations on linear sets.

Example 5.2. For the right shift modulo L, defined on $\mathcal{X} = \{0, ..., L-1\}$ as $\theta_L(\xi) = \xi + 1$ for $\xi = 0, 1, ..., L-2$ and $\theta_L(L-1) = 0$, we find

$$\lambda_{\theta_L} = \frac{2}{L} \ln(L-1).$$

Example 5.3. Define the permutation

$$F_{2l}^{\max}(\xi) = \begin{cases} l + k & \text{if } \xi = 2k \quad 0 \leq k \leq l-1 \\ k & \text{if } \xi = 2k+1 \quad 0 \leq k \leq l-1 \end{cases}$$

on $\mathcal{S} = \{0, ..., 2l-1\}$. The DLE of $F_{2l}^{\max}$ is easily seen to be

$$\lambda_{F_{2l}^{\max}} = \frac{l+1}{2l} \ln l + \frac{l-1}{2l} \ln(l+1) \equiv \lambda_{2l}^{\max}. \tag{12}$$

For large l we have:

$$\lambda_{\theta_{2l}} \approx \frac{1}{l} \log 2l \text{ and } \lambda_{2l}^{\max} \approx \log l.$$

It was proven in [3] that $\lambda_{2l}^{\max}$ is the greatest DLE a bijection on the linear set $\{0, ..., 2l-1\}$ may have. This makes possible to gauge the 'diffusivity' of a permutation of an even number of elements.

Example 5.4. The Advanced Encryption Standard (AES) or Rijndael is a symmetric cipher designed for 128, 192 and 256 bit block lengths [9]; for simplicity, we consider here the first implementation only. In order to calculate the DLE for the AES, we assign to each 128 bit block an integer in $\{0, 1, ..., 2^{128} - 1\}$ via its binary representation. The computation of the DLE has been performed on 7000 iterations of the AES map obtaining DLE = 20.93 after the first round and DLE = 87.22 after the second and subsequent rounds (to be compared to $\lambda_{2^{128}}^{\max} = 88.03$) [1].

Example 5.5. Serpent handles 128-bit messages using a key that can be either 128-, 192-, or 256-bits long [9]. The encryption proceeds basically in 32 rounds, using 8 S-boxes S_i. In the simplest version, the input to the ith round is first XORed with the round key K_i, next each 4-bit subblock is input in parallel into 32 copies of the same S-box $S_{i \bmod 8}$, and finally (except in the last round) the output of the S-boxes is submitted to linear transformations. In order to measure the diffusion property of the whole algorithm, we followed the orbit of a sample of 128-bit random messages. The result is DLE = 84.16 after the first round and DLE = 87.22 (the same as for AES) after the second and subsequent rounds.

6. Spectral properties

We consider here the binary case. The input and the output alphabets are the set $\mathbb{F}_2$ and the internal states set is the n-dimensional vector space $\mathbb{F}_2^n$ over $\mathbb{F}$.

The inverse next-state function is constituted by two functions f'_0 and f'_1, over $\mathbb{F}^n$ and such that $f'_0(s'_t) = f'(s'_t, 0)$ and $f'_1(s'_t) = f'(s'_t, 1)$.

The inverse iterated function $f^{('k)}$ is a function $\mathbb{F}^{n+k} \longrightarrow \mathbb{F}^n$. The Walsh spectrum is a efficient tool to study correlation properties of such vectorial mappings.

By definition, the Walsh matrix of a vectorial function $g : \mathbb{F}^n \longrightarrow \mathbb{F}^m$ is the $2^n \times 2^m$ matrix W_g, with coefficient on line $u \in \mathbb{F}_2^n$ and column

$v \in \mathbb{F}_2^n$ equal to

$$W_g(u,v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{u \cdot g(x) + v \cdot x},$$

where $a \cdot b$ denotes the usual dot product $a_1 b_1 + \cdots + a_n b_n$. The value $W_g(u,v)$ represents the correlation between the function $x \mapsto u \cdot g(x)$ and the linear form $x \longmapsto v \cdot x$.

Remark 3. *The line u of this matrix is the usual Walsh Transform of the Boolean function* $x \mapsto u \cdot g(x)$

The Walsh matrix of the iterated function $f^{(k)}$ may be expressed by mean of the Walsh matrices W_0 and W_1 of the functions f'_0 and f'_1. For u and w in $\mathbb{F}_2^n$ and $v \in \mathbb{F}_2^k$,

$$W_{f^{(k)}}(u, vw) = \frac{1}{2^{nk}} \prod_{i=1}^{k} W_{v_i}(u, w)$$

The synchronizations properties may be expressed by mean of the Walsh matrix. The synchronization delay is less than or equal to D_0 means that the composition of any f'_0 and f'_1 function is a constant function that no longer depends on the initial state s'_{t_0}, and thus that any product of s factors equal to W_0 or W_1 is the Walsh matrix of a constant function.

Statistical synchronization delay may also be expressed by mean of the Walsh matrices. It means that the product of k matrices equal to W_0 or W_1, converges to the Walsh matrix of a constant function for almost all vector $v \in \mathbb{F}^k$, as k grows to infinity.

7. Conclusion

In this paper, self-synchronizing architectures coming from the study of nonlinear dynamics and discrete-time control theory have been presented with the aim of designing devices for cryptographical applications. We have presented properties of dynamical systems namely, invertibility and flatness and their possible use for cryptographic applications. In particular, we have shown that flat dynamical systems may act as self-synchronizing stream ciphers. That may open some new perspectives for construction of such ciphers.

References

[1] J.M. Amigó, J. Szczepanski and L. Kocarev, Discrete chaos and cryptography. In *Proc. of the 2005 International Symposium on Nonlinear Theory and its Applications* (NOLTA'05), p. 461-464, Bruges, Belgium, October 2005 (ISBN 4885522153).

[2] J.M. Amigó, L. Kocarev and J. Szczepanski, Theory and practice of chaotic cryptography, *Phys. Lett. A* **366** (2007) 211-216.

[3] J.M. Amigó, L. Kocarev and J. Szczepanski, Discrete Lyapunov exponent and resistance to differential cryptanalysis, *IEEE Trans. Circ. Syst. II* **54** (2007) 882-886.

[4] J. Fridrich, Symmetric ciphers based on two-dimensional chaotic maps, *Int. J. Bifurcation and Chaos* **8** (1998) 1259–1284.

[5] L. Kocarev, J. Szczepanski, J.M. Amigó and I. Tomovski, Discrete Chaos - Part I: Theory, *IEEE Trans. Circ. and Syst. I* **53** (2006) 1300-1309.

[6] U.M. Maurer, *New Approaches to the Design of Self-Synchronizing Stream Cipher*, Advance in Cryptography, in Proc. Eurocrypt '91, Lecture Notes in Computer Sciences, pp. 548–571, 1991.

[7] G. Millérioux and J. Daafouz. Invertibility and flatness of switched linear discrete-time systems. In *Proc. of the 10th International Conference on Hybrid Systems: Computation and Control (HSCC'07)*, Pisa, Italy, April 2007.

[8] R. L. Devaney. *An introduction to Chaotic Dynamical Systems*. Addison-Wesley, Redwood City, CA, 1989.

[9] J. Pieprzyk, T. Hardjono and J. Seberry, *Fundamentals of Computer Security*. Springer Verlag, Berlin, 2003.

[10] L. Rosier, G. Millérioux and G. Bloch, *Syst. & Control Lett.* **55** (2006) 223.

[11] P. Guillot and S. Mesnager. Nonlinearity and security of self-synchronizing stream ciphers. In *Proc. of the 2005 International Symposium on Nonlinear Theory and its Applications (NOLTA 2005)*, Bruges, Belgium, 18-21 October 2005.

Gilles Millerioux and Jamal Daafouz are partially funded by a grant from the Agence Nationale pour la Recherche in France (Ref. ANR-05-JCJC-0112-01)