Designing Self-Synchronizing Stream Ciphers with Flat Dynamical Systems

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

Designing Self-Synchronizing Stream Ciphers with Flat Dynamical Systems

G. Millérioux, P. Guillot, J.M. Amigó, and J. Daafouz

***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. A special class of dynamical systems, namely the piecewise linear systems, are then considered.**

I. 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 [1] or [2].

The paper is organized as follows. In Sect. II, three important notions related to dynamical systems borrowed from control theory are presented: relative degree, invertibility and flatness. In Sect. III, a connection is established between ciphers defined by flat piecewise linear dynamical systems and self-synchronizing stream ciphers. In Sect. IV, an example of construction of self-synchronizing stream ciphers based on flat dynamical systems is provided.

II. Dynamical systems

A. Basic definition

Definition 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 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 $t \geq 0$

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

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 $t \geq 0$

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

When $\mathcal{D}$ corresponds to a physical process model, all the variables, namely the input, the output and the state belong usually 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. III that considering the three aforementioned 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.

B. Relative degree

Definition 2: The relative degree of the dynamical system $\mathcal{D}$ is the quantity equaling

- 0 if $\exists s_t \in S, \exists a_t, a_t' \in A$ s.t. $h(s_t, a_t) \neq h(s_t, a_t')$

G. Milleerioux and J. Daafouz are with Nancy University, Centre de Recherche en Automatique de Nancy, France
P. Guillot is with Universite Paris 8, France
J. M. Amigo is with Centro de Investigacion Operativa, Universidad Miguel Hernandez de Elche, Alicante

- r if for any sequence $a_{t+i}\cdots a_{t+r}$ $(i>0)$ of input symbols

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

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 thereby considered as 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.

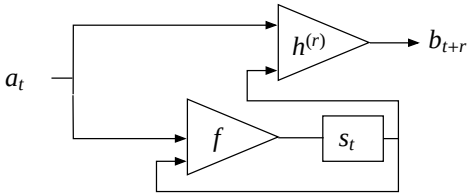

Fig. 1. Block diagram of $\mathcal{D}$

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.

C. 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 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 state $s_t \in S$ and the input sequence $b_t,\ldots,b_{t+R-1}$.
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 $\mathcal{D}^{-1}$ 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.

The next-state i−order iterated inverse function is defined for $i\geq 1$ by $f'^{(i)} : S_R\times B^i \longrightarrow S$ and recursively obeys for $t\geq 0$

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

The i−order iterated inverse next-function has the property that the internal states s_t of the transmitter and the S−component s'_t of the internal state of the receiver fulfill $s'_{t+R+i+1} = f'^{(i+1)}(s'_{t+R}, b_t\cdots b_{t+R-1}, b_{t+R}\cdots b_{t+R+i}) = s_{t+i+1}$ for all $i\geq 0$ if $s'_{t+R} = s_t$ and $s'_{t+t_0+R+i} = s_{t+t_0+i}$ for all $t\geq 0$ if $s'_{t_0+R+i} = s_{t_0+i}$.

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. 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.

D. Flatness

Definition 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 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 $f'^{(i)} : S_R \times B^i \longrightarrow S$. Indeed, 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

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

After performing the change of variable $t \to t - I - 1$, the state reads

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

where * stands for a dummy variable since $f'^{(I+1)}$ does no longer depend on and is only a function $\mathcal{F}$ of $b_{t-I-1} \cdots b_{t+R-1}$. Hence, Eq. (6) gives explicitly the function $\mathcal{F}$, 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. Let us notice that it might be more convenient from a computational point of view to iterate the inverse next-state function rather than resorting to the function $\mathcal{F}$ itself.

III. 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 $d = t_2 - t_1 + 1 = R + I + 1$

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.

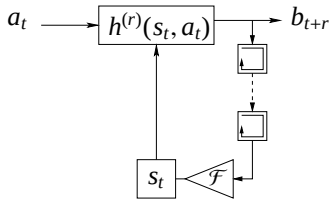

Fig. 2. Self-synchronizing Message-Embedded Stream Cipher

The security of such a canonical self-synchronizing stream cipher is insured as long as the permutation h_{s_t}, when $A = B$, 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 $d = R + I + 1$. As a result, for designing a self-synchronizing stream cipher with statistical synchronization delay, the quantities $R = r$ and/or I must depend on (b_t) and/or s'_t. Regarding cryptographic applications, it may be expected to bring in more complex dynamic.

IV. 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 piecewise linear nonlinearities is provided. The

flatness condition is expressed in terms of algebraic conditions (see [3] 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 $\mathbb{F}$.

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

$$\left\{ \begin{array}{lcl} f(s_t, a_t) = s_{t+1} & = & M_{\sigma(t)} s_t + v_{\sigma(t)} a_t \\ h(s_t, a_t) = b_t & = & C_{\sigma(t)} s_t + D_{\sigma(t)} a_t \end{array} \right. \quad (7)$$

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 $\{M_j\}_{1\le j\le J}$, $\{v_j\}_{1\le j\le J}$, $\{C_j\}_{1\le j\le J}$ and $\{D_j\}_{1\le j\le J}$. The index j corresponds to the discrete mode of the system and results from a switching function $\sigma : t \mapsto j = \sigma(t) \in \{1, \ldots, J\}$.

A. Structural consideration

1) Relative degree: We are checking for an algebraic interpretation of the relative degree for the switched linear system (7) in terms of its state space description matrices. To this end, we must write down the expression of b_{t+i} by iterating (7)

$$b_{t+i} = C_{\sigma(t+i)} M_{\sigma(t)}^{\sigma(t+i-1)} s_t + \sum_{j=0}^{j=i} \mathcal{T}_{\sigma(t)}^{i,j} a_{t+j} \quad (8)$$

with

$$\mathcal{T}_{\sigma(t)}^{i,j} = C_{\sigma(t+i)} M_{\sigma(t+j+1)}^{\sigma(t+i-1)} v_{\sigma(t+j)} \text{ if } j \le i-1, \quad \mathcal{T}_{\sigma(t)}^{i,i} = D_{\sigma(t+i)} \quad (9)$$

and with the transition matrix defined as the product of matrices

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

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

By virtue of (8) and the Definition 2, the following Proposition applies

Proposition 1: The relative degree r of $\mathcal{D}_s$ is

- 0 if for all $t \ge 0$, $\mathcal{T}_{\sigma(t)}^{0,0} \ne 0$;
- the least integer $r < \infty$ such that, for all $t \ge 0$

$$\begin{array}{l} \mathcal{T}_{\sigma(t)}^{i,j} = 0 \text{ for } i = 0, \ldots, r-1 \text{ and } j = 0, \ldots, i \\ \mathcal{T}_{\sigma(t)}^{r,0} \ne 0 \end{array} \quad (10)$$

When (7) has a finite relative degree $r \ge 0$, its output reads at time $t + r$:

$$b_{t+r} = C_{\sigma(t+r)} M_{\sigma(t)}^{\sigma(t+r-1)} s_t + \mathcal{T}_{\sigma(t)}^{r,0} a_t \quad (11)$$

which defines the function $h^{(r)}$ of (3).

2) Left invertibility: If $\mathcal{D}_s$ has a finite relative degree r, the expression of the input a_t is unique and can be deduced from (11):

$$a_t = (\mathcal{T}_{\sigma(t)}^{r,0})^{-1} (b_{t+r} - C_{\sigma(t+r)} M_{\sigma(t)}^{\sigma(t+r-1)} s_t) \quad (12)$$

since the existence of the inverse of $\mathcal{T}_{\sigma(t)}^{r,0}$ is guaranteed. As a result, the following Proposition applies:

Proposition 2: if $\mathcal{D}_s$ has a finite relative degree r, it is left invertible with $R = r$

In other words, if $\mathcal{D}_s$ has a finite relative degree r, the relative degree r of $\mathcal{D}_s$ and its inherent delay R are coincident.

3) Next-state iterated inverse function:

Proposition 3: The next-state iterated inverse function of $\mathcal{D}_s$ is defined for $i \ge 1$ by $f'^{(i)} : S \times B^i \longrightarrow S$ recursively obeying for $t \ge 0$

$$\left\{ \begin{array}{l} s'_{t+R+1} = f'^{(1)}(s'_{t+R}, b_{t+R}) = P_{\sigma(t)} s'_{t+R} + Q_{\sigma(t)} b_{t+R} \\ s'_{t+R+i+1} = f'^{(i+1)}(s'_{t+R}, b_{t+R} \cdots b_{t+R+i}) = \\ P_{\sigma(t+i)} \cdots P_{\sigma(t)} s'_{t+R} + P_{\sigma(t+i)} \cdots P_{\sigma(t+1)} Q_{\sigma(t)} b_{t+R} + \\ \qquad P_{\sigma(t+i)} \cdots P_{\sigma(t+2)} Q_{\sigma(t+1)} b_{t+R+1} + \cdots + \\ P_{\sigma(t+i)} Q_{\sigma(t+i-1)} b_{t+R+i-1} + Q_{\sigma(t+i)} b_{t+R+i} \end{array} \right. \quad (13)$$

with

$$P_{\sigma(t)} = M_{\sigma(t)} - v_{\sigma(t)} (\mathcal{T}_{\sigma(t)}^{r,0})^{-1} C_{\sigma(t+r)} M_{\sigma(t)}^{\sigma(t+r-1)} \quad (14)$$

and

$$Q_{\sigma(t)} = v_{\sigma(t)} (\mathcal{T}_{\sigma(t)}^{r,0})^{-1} \quad (15)$$

Proof: On one hand, substituting (11) into (13) and taking into account that $r = R$ yields:

$$\begin{array}{rcl} f'^{(1)}(s'_{t+R}, b_{t+R}) & = & s'_{t+R+1} \\ & = & P_{\sigma(t)} s'_{t+R} + \\ & & v_{\sigma(t)} (\mathcal{T}_{\sigma(t)}^{R,0})^{-1} C_{\sigma(t+R)} M_{\sigma(t)}^{\sigma(t+R-1)} s_t + \\ & & v_{\sigma(t)} (\mathcal{T}_{\sigma(t)}^{R,0})^{-1} \mathcal{T}_{\sigma(t)}^{R,0} a_t \end{array} \quad (16)$$

Taking into account (14) and noticing that $(\mathcal{T}_{\sigma(k)}^{R,0})^{-1} \mathcal{T}_{\sigma(k)}^{R,0} = 1$, if $s'_{t+R} = s_t$ then:

$$s'_{t+R+1} := M_{\sigma(t)} s'_{t+R} + v_{\sigma(t)} a_t = M_{\sigma(t)} s_t + v_{\sigma(t)} a_t \quad (17)$$

Hence, $s'_{t+i+R+1} = f'^{(i+1)}(s'_{t+R}, b_{t+R} \cdots b_{t+R+i}) = s_{t+i+1}$ for all $t \ge 0$, which is the definition of the iterated inverse next-function.

■

Proposition 4: The inverse output function $h' : S \times B \longrightarrow A$ is given by

$$a'_{t+R} = h'(s'_{t+R}, b_{t+R}) = (\mathcal{T}_{\sigma(t)}^{R,0})^{-1} (b_{t+R} - C_{\sigma(t+R)} M_{\sigma(t)}^{\sigma(t+R-1)} s'_{t+R}) \quad (18)$$

Proof: The proof is immediate since by letting $s'_{t+R} = s_t$ in (18), the comparison with (12) yields $a'_{t+R} = a_t$.

■

4) Flatness: We now derive an algebraic interpretation of flat outputs for (7).

Proposition 5: The output of (7) assumed to be left invertible, is a flat output if there exists a positive integer $I < \infty$ such that for all $t \geq 0$

$$P_{\sigma(t+I)} \cdots P_{\sigma(t)} = \mathbf{0} \tag{19}$$

where $\mathbf{0}$ stands for the null matrix.

Proof: Take into account the next-iterated inverse function (13). Assume that there exists an integer I such that (19) is fulfilled. Thus $s'_{t+R+I+1} = s_{t+I+1}$ does no longer depend on the state s'_{t+R} but on a finite number of forward/backward iterated output b_t of $\mathcal{D}_s$. Thus, according to Definition 4, b is a flat output.

■

5) Self-synchronous stream ciphers flatness-based design: Let $\mathcal{P}$ be the sets of possible matrices $P_{\sigma(t+I)} \cdots P_{\sigma(t)}$.

Proposition 6: The system $\mathcal{D}_s$ 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 flat dynamical systems can be extended to dynamical systems with non-linear transitions.

B. Behavioral consideration

We have seen in Sect. II-C that when, as usual, the input alphabet A and the output alphabet B are the same, the output functions $h_{s_t}^{(r)} : a_t \mapsto h^{(r)}(s_t, a_t)$ are a family of permutations of A, parameterized by the internal states s_t. 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 orbits $\{f^n(x) : n \in \mathbb{N}\}$ have random-like properties for 'typical' choices of $x \in X$ (see [5] for a formal definition of chaos). For cryptographic purposes, we take 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 [6]. The main tool of discrete chaos is the discrete Lyapunov Exponent.

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. 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 [7]. These maps have the nice property that the precision of the initial point does not degrade along its orbit. See [8] for a general view of digital chaotic cryptography.

V. 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 three notions related to dynamical systems, namely relative degree, invertibility and flatness. We have shown that insofar as a dynamical system has a finite relative degree, is left invertible and flat, it may act as self-synchronizing stream cipher. That may open some new perspectives for construction of such ciphers.

Acknowledgment

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)

References

[1] U. M. Maurer. New approaches to the design of self-synchronizing stream cipher. *Advance in Cryptography, In Proc. Eurocrypt '91, Lecture Notes in Computer Science*, pages 548–471, 1991.

[2] J. Daemen and P. Kitsos. The self-synchronizing stream cipher moustique. *eSTREAM, ECRYPT Stream Cipher Project*, June 2005. Available online at http://www.ecrypt.eu.org/stream.

[3] G. Millerioux 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.

[4] J. Fridrich. Symmetric ciphers based on two-dimensional chaotic maps. *International Journal of Bifurcation and Chaos*, 8(6):1259 – 1284, June 1998.

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

[6] L. Kocarev, J. Szczepanski, J. M Amigo, and I. Tomosvski. Discrete chaos: part i. *IEEE Trans. on Circuits and Systems I*, 53, 2006.

[7] L. Rosier, G. Millerioux, and G. Bloch. Chaos synchronization for a class of discrete dynamical systems on the $n-$ dimensional torus. *Systems and control letters*, 55:223–231, 2006.

[8] L. Kocarev J.M. Amigo and J. Szczepanski. Theory and practice of chaotic cryptography. *Phys. Lett. A*, 366:211–216, 2007.