A constructive approach for the design of self-synchronizing dynamical systems: an application to communications

Jeremy Parriaux, Gilles Millérioux

A constructive approach for the design of self-synchronizing dynamical systems: an application to communications

Jérémy Parriaux * **Gilles Millérioux** *

* *Nancy University*
Research Center for Automatic Control of Nancy (CRAN UMR 7039)
2 rue Jean Lamour, 54519 Vandoeuvre-les-Nancy, France,
(e-mail: jeremy.parriaux@esstin.uhp-nancy.fr,
gilles.millerioux@esstin.uhp-nancy.fr)

Abstract: This paper addresses the problem of self-synchronization of dynamical systems in a so-called master-slave configuration. The study is motivated by potential cryptographic applications. It is shown that the notion of flatness is central for guaranteeing self-synchronization and that the concept of transmissions zeros plays also an important role. We motivate the fact that switched linear systems have great interest in this context.

Keywords: switched systems, synchronization, communication, flatness, invertibility

1. INTRODUCTION

Synchronization of dynamical systems is an important purpose in many fields like biology, mechanics, communications. Synchronization means coordinated behavior of different interconnected entities involved in an overall system. Many different definitions and related configurations, in terms of coupling, can be investigated. An exhaustive and interesting overview can be found in Blekhman et al. [1997]. A special kind of synchronization is the self-synchronization. By self-synchronization, it is meant a coordinated behavior which is achieved without any external control.

The configuration under consideration in this paper involves two parties: a so-called master system which forces, through a unidirectional coupling, a second system called slave. The configuration is borrowed from the field of communications and more specifically secure transmissions. In this context, cryptography plays a central role. It is the discipline which is mainly intended to protect information and to guarantee confidential exchanges through public channels. One of the cryptographic methods obeys the following principle. The transmitter, called the cipher, delivers a complex sequence (theoretically indistinguishable from a uniformly random sequence) used to conceal information. The information to be kept secret is, in some sense, "mixed" with the complex sequence so that the resulting sequence called cryptogram, which is conveyed to the receiver, cannot be understood by any unauthorized party. For proper information recovery, the receiver, called the decipher, must deliver the same complex sequence synchronized with the cipher. It is typically a master-slave configuration with unidirectional coupling. The master is nothing but the cipher, the slave is nothing but the decipher. The coupling is achieved through the cryptograms. Some communication setups require that the synchronization must be guaranteed without any external control. In other words, self-synchronization must be achieved. Such a requirement can be motivated by the fact that, for instance, insertion of synchronization flags in the transmitted packets is forbidden for throughput purposes.

From the 90's, many "scrambling" methods resorting to synchronized dynamical systems have been proposed. A recent overview can be found in Banerjee [2010]. However, their well admitted poor efficiency regarding the security can be explained by the fact that they were disconnected from standard ciphering methods. Recently, in Millérioux et al. [2008] and Millérioux and Guillot [2010], the connection has been made and shows that using dynamical systems in a master-slave configuration makes sense from a cryptographic point of view under specific conditions. In particular, whenever the involved dynamical systems are flat, the communication scheme is structurally equivalent to a so-called self-synchronizing stream cipher. So far, the study reduced to analysis, no efficient constructive approach for the design was proposed. The aim of the present work is precisely to handle this problem. Discrete-time switched linear systems are specifically addressed because they correspond to the so-called Maiorana McFarland construction which has proved to produce functions that have many interesting cryptographic properties (see Carlet [2010]).

The outline of this paper is the following. In Section 2, strict necessary background on cryptography is provided. A special emphasis is put on the role of self-synchronization in this context and a formal definition of finite-time self-synchronization is given. In Section 3, the design of admissible master-slave configurations, described by piecewise linear systems, achieving finite-time

⋆ This work was supported in part by the Institut des Sciences et de l'Ingénierie des Systèmes, Centre National de la Recherche Scientifique, Programmes Exploratoires Pluridisciplinaires (PEPS), Projet Autocrypt

self-synchronization is detailed. A constructive approach for guaranteeing the self-synchronization is suggested. It is mainly based on the notion of nilpotent semigroups. A connection between the issue of guaranteeing self-synchronization and the concept of flatness is brought out. Further considerations for the design are developed in Section 4 where it is shown that the concept of transmission zeros of a dynamical system play an important role. Finally, Section 5 is devoted to an example.

Notation $\mathbf{1}_n$ stands for the identity matrix of dimension n, $\mathbf{0}$ stands for the zero matrix of appropriate dimension regarding the situation. We denote by $\{z\}_{k_1}^{k_2}$ the sequence $\{z_{k_1}, \ldots, z_{k_2}\}$ when the initial and final times k_1 and k_2 are defined, otherwise the sequence is merely denoted $\{z\}$.

2. CRYPTOGRAPHY AND SYNCHRONIZATION

2.1 Background on cryptography

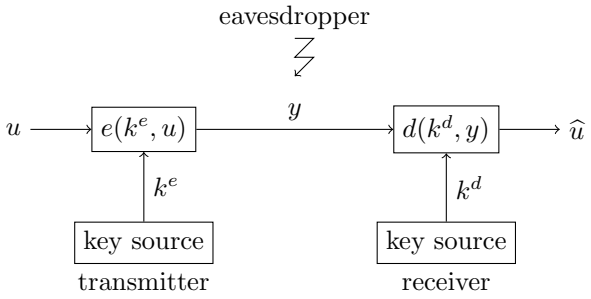

Fig. 1. General encryption mechanism

A general encryption mechanism, also called cryptosystem or cipher, is illustrated in Fig. 1. We are given an alphabet A, that is, a finite set of basic elements named symbols. On the *transmitter* part, a plaintext (also called information or message) $\{u\} \in \mathcal{U}$ ($\mathcal{U}$ is called the message space) consisting of a string of symbols $u_k \in A$ is encrypted according to an encryption function e which depends on the key $k^e \in \mathcal{K}$ ($\mathcal{K}$ is called the key space). The resulting ciphertext $\{y\} \in \mathcal{C}$ ($\mathcal{C}$ is called the ciphertext space), a string of symbols y_k from an alphabet B usually identical to A, is conveyed through a public channel to the *receiver*. At the receiver side, the ciphertext y_k is decrypted according to a decryption function d which depends on the key $k^d \in \mathcal{K}$. For a prescribed k^e, the function e must be invertible. Cryptography distinguishes asymmetric and symmetric ciphers. Asymmetric cryptography is largely based upon computationally very demanding mathematical problems, for instance, integer factorization into primes. It is not discussed in this paper. In symmetric encryption, both keys are identical, that is $k^d = k^e$. That explains the terminology "symmetric".
Next we describe a special class of symmetric ciphers, under consideration hereafter, called stream ciphers, for which synchronization is a central issue. It is shown that the problem can be tackled with efficiency through the control theory point of view.

For stream ciphers, the key k^e and k^d are replaced by a time-varying sequence called *running key* or *keystream*. They are denoted $\{x\}$ (with samples x_k) at the transmitter part and $\{\widehat{x}\}$ (with samples $\widehat{x}_k$) at the receiver part. As a result, stream ciphers require keystream generators. The keystreams $\{x\}$ and $\{\widehat{x}\}$ are produced by deterministic dynamical systems and must be synchronized. The secret key k^e is some suitable selected parameters of the dynamical systems, the selection being based on security considerations. As mentioned in the introduction, some applications require that the synchronization is guaranteed without any external control that is, self-synchronization must be achieved. In such a case, the stream ciphers must have a special architecture and they are called Self-Synchronizing Stream Ciphers. An overview on this class of ciphers can be found in Millérioux and Guillot [2010], Daemen and Kitsos [2005].

2.2 Self-synchronization and ciphering

Self-Synchronizing Stream Ciphers (written hereafter SSSC for short) admit at the transmitter and receiver ends the respective equations:

$$\begin{cases} x_k = g_{k^e}(y_{k-K}, \ldots, y_{k-1}) \\ y_k = e(x_k, u_k) \end{cases} \tag{1}$$

$$\begin{cases} \widehat{x}_k = g_{k^e}(y_{k-K}, \ldots, y_{k-1}) \\ \widehat{u}_k = d(\widehat{x}_k, y_k) \end{cases} \tag{2}$$

g_{k^e} is the function that generates the keystreams $\{x\}$ and $\{\widehat{x}\}$. It depends on K past values of y_k.

The ciphertext y_k is worked out through an encryption function e which must be invertible for any prescribed x_k. The decryption is performed through a function d depending on the ciphertext y_k and on the running key $\widehat{x}_k$ of the receiver. Such a function must obey the rule:

$$\widehat{u}_k = d(\widehat{x}_k, y_k) = u_k \text{ if } \widehat{x}_k = x_k \tag{3}$$

According to (3), the synchronization of the keystreams $\{x\}$ and $\{\widehat{x}\}$ generated respectively at the transmitter and receiver sides is a condition for proper decryption. Since the function g_{k^e} is identical at the transmitter and receiver sides and shares the same arguments, namely the past ciphertexts y_{k-i} $(i = 1, \ldots, K)$, it is clear that the generators synchronize automatically after a finite transient time of length K. This kind of self-synchronization is called finite time self-synchronization.

Actually, the model (1)–(2) of an SSSC is a conceptual model, called canonical representation, that can correspond to different architectures. It turns out that resorting to dynamical systems instead of implementing directly the canonical function g_{k^e} is much more relevant for two major reasons (some detailed motivations can be found in Maurer [1991] and Daemen [1995]). First, implementation of a complex function in a recursive way is, in general, much more computationally efficient than implementing the function itself. Secondly, the canonical representation (1)–(2) assumes that the synchronization delay K is bounded. This assumption limits the complexity of the ciphering which can be represented as a memoryless function. This requirement is not mandatory in practice, and it is acceptable that the synchronization delay is not a constant value but a random variable with a probability law that reaches one as time reaches infinity. In this case, self-synchronization is said to be statistical. Statistical

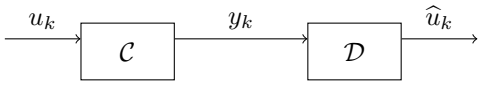

Fig. 2. Dynamical system-based cryptosystems

self-synchronization is more general than the finite-time one. Its interest lies in a broader choice of candidate dynamical systems. The resulting flexibility is important in view of matching additional constraints, besides the self-synchronization, in particular regarding the security of the communication setup. Statistical self-synchronization is not addressed in the present paper, it is detailed for the Boolean case in Parriaux et al. [2010].

To sum up, the problem can be formulated as follows. We are given a setup with two parts (Fig. 2). The first part consists of a dynamical system $\mathcal{C}$, with input u_k (playing the role of the plaintext), output y_k (playing the role of the ciphertext) and state vector x_k (playing the role of the keystream).

$$\mathcal{C} \begin{cases} x_{k+1} = f(x_k, u_k) \\ y_k \quad\;\; = h(x_k, u_k) \end{cases} \tag{4}$$

The output y_k ensures a unidirectional coupling with the second part, the dynamical system $\mathcal{D}$ with state vector $\widehat{x}_k$. It acts as an input for $\mathcal{D}$.

$$\mathcal{D} \begin{cases} \widehat{x}_{k+1} = \widehat{f}(\widehat{x}_k, y_k) \\ \widehat{u}_k \quad\;\; = \widehat{h}(\widehat{x}_k, y_k) \end{cases} \tag{5}$$

$\widehat{u}_k$ is the output of $\mathcal{D}$. In a cryptographic context, it acts as the recovered information and must be equal to u_k whenever $x_k = \widehat{x}_k$.

Definition 1. (Finite time self-synchronization). The unidirectional coupled system $\mathcal{C}$–$\mathcal{D}$ is finite time self-synchronizing if, for all admissible input sequences,

$$\exists K \in \mathbb{N},\, \forall x_0,\, \widehat{x}_0,\, \forall k \geq K,\; x_k = \widehat{x}_k \tag{6}$$

A delay $r \in \mathbb{N}$ can be allowed. If so, Equation (6) turns into

$$\exists K \in \mathbb{N},\, \forall x_0,\, \widehat{x}_0,\, \forall k \geq K,\; x_k = \widehat{x}_{k+r} \tag{7}$$

Finally, the issue to be investigated is the following. How to design a master-slave setup $\mathcal{C}$–$\mathcal{D}$ so that

- self-synchronization (6) (possibly (7)) can be guaranteed
- proper input recovery $\widehat{u}_k = u_k$ is ensured whenever self-synchronization is achieved

It is the purpose of the next sections. Actually, as motivated in the introduction, we concentrate on the special class of switched linear systems.

3. FINITE TIME SELF-SYNCHRONIZATION AND SWITCHED SYSTEMS

The equations of the set-up read at the transmitter part

$$\mathcal{C} \begin{cases} x_{k+1} = A_{\sigma(k)} x_k + B_{\sigma(k)} u_k \\ y_k \quad\;\; = C_{\sigma(k)} x_k + D_{\sigma(k)} u_k \end{cases} \tag{8}$$

and at the receiver part

$$\mathcal{D} \begin{cases} \widehat{x}_{k+1} = A'_{\sigma(k)} \widehat{x}_k + B'_{\sigma(k)} y_k \\ \widehat{u}_k \quad\;\; = C'_{\sigma(k)} \widehat{x}_k + D'_{\sigma(k)} y_k \end{cases} \tag{9}$$

with $u_k, \widehat{u}_k \in \mathbb{F}$, $y_k \in \mathbb{F}$ and $x_k, \widehat{x}_k \in \mathbb{F}^n$ where $\mathbb{F}$ is a field. In digital transmissions, $\mathbb{F}$ is a finite field of cardinality p^q with p a prime and q a positive integer. When $q = 1$, all the operations, namely, addition, subtraction, multiplication and inversion are still defined like in the field of real numbers except that the results are computed modulo p.

The switching function σ is defined as

$$\sigma : k \in \mathbb{N} \mapsto j = \sigma(k) \in \{1, \ldots, J\} = \mathcal{J}$$

At a given time k, the index j corresponds to the mode of the system given by the switching function σ. J is the number of modes. All the matrices, namely $A_{\sigma(k)} \in \mathbb{F}^{n\times n}$, $B_{\sigma(k)} \in \mathbb{F}^{n\times 1}$, $C_{\sigma(k)} \in \mathbb{F}^{1\times n}$ and $D_{\sigma(k)} \in \mathbb{F}$ belong to the respective finite sets $(A_j)_{1\leq j\leq J}$, $(B_j)_{1\leq j\leq J}$, $(C_j)_{1\leq j\leq J}$ and $(D_j)_{1\leq j\leq J}$. The switching function must depend on the output y_k. The motivation of such a dependence lies in that the switching rule is the same for both systems $\mathcal{C}$ and $\mathcal{D}$ and must be self-synchronizing. Thus, it must depend on shared variables and so on the output y_k or a finite sequence of delayed outputs. It is worth pointing out that the writing $\sigma(k)$ is somehow abusive since the dynamical system is not a time-varying system. We denote by $\{v\}$ the sequence of modes $\{v\} = \{\sigma(0), \sigma(1), \ldots\}$. If the sequence has a finite length K, it is an element of the set denoted $\mathcal{J}^K$.
In the following, we derive conditions for guaranteeing self-synchronization of the master-slave set-up $\mathcal{C}$–$\mathcal{D}$ (8)–(9) and propose constructive approaches for achieving finite-time self-synchronization.

3.1 General conditions

Theorem 1. The set-up (8)–(9) is finite-time self-synchronizing whenever the three following conditions are fulfilled:

- $\forall j \in \mathcal{J},\; D'_j \neq 0$ (10)
- $\exists K \in \mathbb{N}, \forall x_0,\, \widehat{x}_0,\, \forall \{v\} \in \mathcal{J}^K,\; \prod_{i=0}^{K-1} A'_{v_i} = 0$ (11)
- Given the matrices (A'_j, B'_j, C'_j, D'_j) of $\mathcal{D}$, the system $\mathcal{C}$ reads

$$\begin{cases} x_{k+1} = \left(A'_{\sigma(k)} - B'_{\sigma(k)} (D'_{\sigma(k)})^{-1} C'_{\sigma(k)}\right) x_k \\ \qquad\quad + B'_{\sigma(k)} (D'_{\sigma(k)})^{-1} u_k \\ y_k \quad\;\; = -(D'_{\sigma(k)})^{-1} C'_{\sigma(k)} x_k + (D'_{\sigma(k)})^{-1} u_k \end{cases} \tag{12}$$

Proof 1. Since $D'_j \neq 0$ for any $j \in \mathcal{J}$ (Condition (10)), the input u_k can be derived from the output equation of $\mathcal{C}$ and reads

$$u_k = D'_{\sigma(k)} y_k + C'_{\sigma(k)} x_k \tag{13}$$

Thus,

$$\begin{aligned} \widehat{u}_k - u_k &= C'_{\sigma(k)} \widehat{x}_k + D'_{\sigma(k)} y_k - D'_{\sigma(k)} y_k \\ &\quad - C'_{\sigma(k)} x_k \\ &= C'_{\sigma(k)} (\widehat{x}_k - x_k) \end{aligned}$$

Let the reconstruction error be $\epsilon_k = \widehat{x}_k - x_k$. Then, from (9) and (12)

$$
\begin{aligned}
\epsilon_{k+1} &= A'_{\sigma(k)}\widehat{x}_k + B'_{\sigma(k)}y_k \\
&\quad -(A'_{\sigma(k)} - B'_{\sigma(k)}(D'_{\sigma(k)})^{-1}C'_{\sigma(k)})x_k \\
&\quad -B'_{\sigma(k)}(D'_{\sigma(k)})^{-1}u_k \\
&= A'_{\sigma(k)}\epsilon_k - B'_{\sigma(k)}(y_k - (D'_{\sigma(k)})^{-1}u_k) \\
&\quad -B'_{\sigma(k)}(D'_{\sigma(k)})^{-1}u_k + B'_{\sigma(k)}y_k \\
&= A'_{\sigma(k)}\epsilon_k
\end{aligned}
\tag{14}
$$

After iterating (14) K times and taking into account (11), $\epsilon_k = 0$ or equivalently $x_k = \widehat{x}_k$ for any $k \geq K$. Hence, according to Definition 1, the set-up (8)–(9) is finite-time self-synchronizing. That completes the proof.

No constraint is imposed on B'_j and C'_j. Condition (11) means that regardless of the order of multiplication of the matrices A'_j, and so for any mode sequences, the product is zero after a finite number K of iterations. K is the delay of synchronization.

Remark 1. The condition $D'_j \neq 0$ for any $j \in \mathcal{J}$ means that the relative degree of the systems $\mathcal{C}$ and $\mathcal{D}$ is zero.

Remark 2. The system (8) is a right inverse for the system (9). Indeed, for any identical initial conditions $x_0 = \widehat{x}_0$ and for any identical mode sequence $\{v\}$, the system (8) drives (9) such that $\forall k \geq 0$, $\widehat{u}_k = u_k$.

Theorem 1 does not provide a constructive solution for the selection of appropriate matrices A'_j which must fulfill the constraint (11). The purpose of the next paragraph is to obtain an equivalent constructive condition. It is based on the notion of nilpotent semigroups.

3.2 Constructive approach

Let us first recall two definitions:

Definition 2. (Semigroup). A semigroup $\mathcal{S}$ is a set together with an associative internal law. It is said to be finite if $\mathcal{S}$ has a finite number of elements.

Definition 3. (Nilpotent semigroup). A semigroup $\mathcal{S}$ is said to be nilpotent if it is such that any product of a finite number $t \in \mathbb{N}^*$ of its elements (possibly the same element) is always 0. The smallest integer t is called the class of nilpotency of $\mathcal{S}$.

Proposition 1. In order for (11) to be fulfilled, the set of dynamical matrices $\{A'_j,\ j \in \mathcal{J}$ must generate a nilpotent semigroup. The delay of synchronization K equals the class of nilpotency of this semigroup.

A theorem, useful for the construction of semigroups with a given class of nilpotency is stated in the book Radjavi and Rosenthal [2000] and recalled below.

Theorem 2. (Levitsky's theorem). Any semigroup of nilpotent matrices can be triangularized.

In other words, there is a common basis in which all the matrices of the semigroup are upper triangular with zeros on the diagonal.

Remark 3. The product of t nilpotent matrices which commute pairwise is 0 but the product of t nilpotent matrices is not, in general, nilpotent. Indeed, we observe that $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. Theorem 2 provides a generalization of this special case, should each matrix be nilpotent is only a necessary condition.

Hence, based on Levitsky's theorem, the construction of the family $(A'_j)_{1\leq j\leq J}$ which fulfills (11) follows three successive steps

- choose an invertible matrix $T \in \mathbb{F}^{n\times n}$
- choose a set of J upper triangular matrices $\bar{A}'_j$ with zero on the diagonal
- for all $j \in \mathcal{J}$, compute $A'_j = T^{-1}\bar{A}'_j T$

The matrix T may possibly be the identity matrix.

Remark 4. Because of Levitzky's theorem, the consideration of a semigroup of n–dimensional matrices is equivalent to the consideration of the corresponding set of upper triangular matrices. And yet, for triangular matrices, it is clear that the nilpotency class is at most n. As a result, the delay of synchronization K is upper bounded by n.

3.3 Connection with flatness

Flatness is an important concept in control theory. It was introduced in Fliess et al. [1995] and a deep insight can be found in the book Sira-Ramirez and Agrawal [2004]. In this section, we show that the constructive approach proposed for designing a finite-time self-synchronizing master-slave system amounts to designing a flat system $\mathcal{C}$ with flat output y_k.

Definition 4. (Flat dynamical system). A system with input u_k and state vector x_k is said to be flat if there is a set of independent variables y_k, referred to as flat output, such that all the system variables can be expressed as a function of the flat output and a finite number of its backward and/or forward iterates. In particular, there exist two functions $\mathcal{F}$ and $\mathcal{G}$ such that

$$
\begin{cases}
x_k = \mathcal{F}(y_{k+t_1}, \ldots, y_{k+t_2}) \\
u_k = \mathcal{G}(y_{k+t'_1}, \ldots, y_{k+t'_2})
\end{cases}
$$

where $t_1, t_2, t'_1, t'_2 \in \mathbb{Z}$.

Proposition 2. The system $\mathcal{C}$ resulting from the conditions (10)-(11)-(12) is flat with flat output y_k

Proof 2. The state of the switched system (9) can be written, at time $k+K$

$$
\begin{aligned}
\widehat{x}_{k+K} &= \prod_{i=0}^{K-1} A'_{\sigma(k+K-1-i)}\widehat{x}_k \\
&\quad + \sum_{i=0}^{K-1}\left[\prod_{j=i+1}^{K-1} A'_{\sigma(k+K-j)}\right] B'_{\sigma(k+i)}y_{k+i}
\end{aligned}
$$

Therefore, if (11) holds, any state at time $k \geq 0$ reads:

$$
\widehat{x}_{k+K} = \sum_{i=0}^{K-1}\left[\prod_{j=i+1}^{K-1} A'_{\sigma(k+K-j)}\right] B'_{\sigma(k+i)}y_{k+i} \tag{15}
$$

And yet, $\epsilon_k = 0$ or equivalently $x_k = \widehat{x}_k$ for any $k \geq K$. Hence, after a shift of K, one obtains

$$\widehat{x}_k = x_k = \sum_{i=0}^{K-1} \left[\prod_{j=i+1}^{K-1} A'_{\sigma(k-j)} \right] B'_{\sigma(k-K+i)} y_{k-K+i} \quad (16)$$

which gives the function $\mathcal{F}$.
On the other hand, since $D'_j \neq 0$ for any $j \in \mathcal{J}$, the input u_k reads like (13). Substituting the expression (16) of x_k into (13) gives the function $\mathcal{G}$. That completes the proof.

Relation (16), and in the general case, the function $\mathcal{F}$, gives explicitly the function g_{k^e} of (1) and (2). As a result, and as pointed out in Section 2.2, there is an equivalence between the recursive part of both equations (4) and (5) and the function $\mathcal{F}$. The equivalence applies under flatness conditions. In the special case of switched linear systems, (8) and (9) can be equivalently rewritten into the respective canonical forms (1) and (2)

$$\begin{cases} x_k = \displaystyle\sum_{i=0}^{K-1} \left[\prod_{j=i+1}^{K-1} A'_{\sigma(k-j)} \right] B'_{\sigma(k-K+i)} y_{k-K+i} \\ y_k = C_{\sigma(k)} x_k + D_{\sigma(k)} u_k \end{cases} \quad (17)$$

$$\begin{cases} \widehat{x}_k = \displaystyle\sum_{i=0}^{K-1} \left[\prod_{j=i+1}^{K-1} A'_{\sigma(k-j)} \right] B'_{\sigma(k-K+i)} y_{k-K+i} \\ \widehat{u}_k = C'_{\sigma(k)} \widehat{x}_k + D'_{\sigma(k)} y_k \end{cases} \quad (18)$$

It is worth pointing out that, from a computational point of view, the recursive form (8)–(9) is more relevant than (17)–(18)

4. TRANSMISSION ZEROS AND SURJECTIVITY

For cryptographic purposes (basically a consideration regarding the entropy of sequences), it is relevant that the maps $x_k \mapsto A_j x_k$ $j \in \mathcal{J}$ are surjective. In other words, we want to guarantee that

$$\forall j \in \mathcal{J}, \ \operatorname{rank}(A_j) = n \quad (19)$$

The problem lies in that, according to Theorem 1, the matrices (A_j, B_j, C_j, D_j) of the system $\mathcal{C}$ are not designed directly but are derived from (A'_j, B'_j, C'_j, D'_j) of $\mathcal{D}$. Hence, we must find out a condition on the matrices (A'_j, B'_j, C'_j, D'_j) so that (19) is ensured. It turns out that the notion of *transmission zeros* are relevant to this end.

A definition of transmission zeros can be found for example in Schrader and Sain [1989]. It is recalled below and particularized for a SISO system.

Definition 5. Let us consider a SISO linear system with state space realization (A, B, C, D). The *transmission zeros* are the complex numbers $\{s_i\}$ which satisfy

$$\operatorname{rank} \begin{bmatrix} A - s_i \mathbf{1}_n & B \\ C & D \end{bmatrix} < n + 1 \quad (20)$$

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

Before proceeding further, we must introduce some notation. Consider the matrix T and the corresponding matrices $A'_j = T^{-1} \bar{A}'_j T$ derived from $\bar{A}'_j$ $(j \in \mathcal{J})$ as explained in Section 3.2 devoted to the constructive approach.

Let us write $\bar{A}'_j$ as

$$\bar{A}'_j = \begin{bmatrix} 0 & a_j^1 & & \\ & 0 & a_j^2 & A_j^* \\ & & \vdots & \ddots \\ & \mathbf{0} & & 0 \quad a_j^{n-1} \\ & & \cdots & 0 \end{bmatrix} \quad (21)$$

where A_j^* denotes the coefficients above the $n-1$ diagonal entries a_j^m $(m = 1, \ldots, n-1)$ located above the zero diagonal. Let have

$$TB'_j = [b_j^1 \cdots b_j^n]^T \quad (22)$$

b_j^m stands for the m^{th} component of the column vector TB'_j.

$$C'_j T^{-1} = [c_j^1 \cdots c_j^n] \quad (23)$$

c_j^m stands for the m^{th} component of the row vector $C'_j T^{-1}$.

Proposition 3. The surjectivity of each map $x_k \mapsto A_j x_k$ $(j \in \{1, \ldots, J\})$ of $\mathcal{C}$ is guaranteed whenever

$$c_j^1 b_j^n \prod_{m=1}^{n-1} a_j^m \neq 0 \quad (24)$$

Proof 3. According to Remark 2, $\mathcal{C}$ is a right inverse for $\mathcal{D}$. Furthermore, let us recall that (see Remark 1) the relative degree of $\mathcal{C}$ and $\mathcal{D}$ is zero. We conclude that each realization (A'_j, B'_j, C'_j, D'_j) $(j \in \mathcal{J})$ of $\mathcal{D}$ has n transmission zeros s_i and the s_i's are nothing but the n eigenvalues λ_i of A_j of $\mathcal{C}$. They are the roots of

$$\Psi_j(s) = \det \ R = 0 \ \text{ with } \ R = \begin{bmatrix} A'_j - s\mathbf{1}_n & B'_j \\ C'_j & D'_j \end{bmatrix} \quad (25)$$

R is often called the Rosenbrock's matrix.
$\Psi_j(s)$ is a polynomial, its constant monomial is $\Psi_j(0)$ and corresponds to the product $\prod_{i=1}^n$ of the roots of $\Psi_j(s)$ and so corresponds to the product $\prod_{i=1}^n \lambda_i$ of the eigenvalues of A_j of $\mathcal{C}$. Hence, surjectivity of $x_k \mapsto A_j x_k$ $j \in \mathcal{J}$ is guaranteed whenever $\Psi_j(0) \neq 0$.

The following equalities apply

$$\begin{aligned} \Psi_j(0) &= \det \begin{bmatrix} A'_j & B'_j \\ C'_j & D'_j \end{bmatrix} = \det \begin{bmatrix} T^{-1} \bar{A}'_j T & B'_j \\ C'_j & D'_j \end{bmatrix} \\ &= \det \left(\begin{bmatrix} T^{-1} & \mathbf{0} \\ \mathbf{0} & 1 \end{bmatrix} \begin{bmatrix} \bar{A}'_j & TB'_j \\ C'_j T^{-1} & D'_j \end{bmatrix} \begin{bmatrix} T & \mathbf{0} \\ \mathbf{0} & 1 \end{bmatrix} \right) \\ &= \det \begin{bmatrix} \bar{A}'_j & TB'_j \\ C'_j T^{-1} & D'_j \end{bmatrix} \end{aligned} \quad (26)$$

Consider a partitioned matrix with four sub-blocks E, F, G, H of compatible dimensions. We recall a result concerning its determinant.

$$\det \begin{bmatrix} E & F \\ G & H \end{bmatrix} = \det(H) \cdot \det(E - FH^{-1}G)$$

Taking into account the special structure (21) of $\bar{A}'_j$, (22) and (23), it turns out that basic manipulations yield

$$\Psi_j(0) = \det \begin{bmatrix} \bar{A}'_j & TB'_j \\ C'_j T^{-1} & D'_j \end{bmatrix} = c_j^1 b_j^n \prod_{m=1}^{n-1} a_j^m \quad (27)$$

That completes the proof.

5. EXAMPLE

This section gives an example that illustrates the construction of a finite-time self-synchronizing setup. We propose to design a finite time self-synchronizing system of dimension $n = 3$ and with $J = 3$ modes. We consider matrices defined over the finite field $\mathbb{F} = \mathbb{Z}/7\mathbb{Z}$. This means that the only coefficients allowed for the matrices are elements in the set $\{0, \ldots, 6\}$ and that the operations of additions and multiplications are performed modulo 7.

The design starts with the setting of the matrices A'_j, B'_j, C'_j, D'_j which must fulfill the three conditions of Theorem 1, the condition (11) being replaced by the constructive approach provided in Section 3.2. We add the condition (24) on surjectivity.

First, for simplicity, we choose $D'_j = 1$ for any $j \in \{1, 2, 3\}$. Secondly, we choose a set of three 3–dimensional matrices $\bar{A}'_j$ in the form of strict upper triangular matrices and with non zero entries located above the diagonal in order to guarantee the surjectivity.

$$\bar{A}'_1 = \begin{pmatrix} 0 & 3 & 2 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \bar{A}'_2 = \begin{pmatrix} 0 & 2 & 1 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix} \bar{A}'_3 = \begin{pmatrix} 0 & 1 & 3 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix}$$

We then choose an invertible matrix T

$$T = \begin{pmatrix} 4 & 0 & 5 \\ 1 & 5 & 2 \\ 5 & 5 & 5 \end{pmatrix}$$

Its inverse over $\mathbb{F} = \mathbb{Z}/7\mathbb{Z}$ reads

$$T^{-1} = \begin{pmatrix} 4 & 2 & 5 \\ 6 & 1 & 2 \\ 4 & 4 & 3 \end{pmatrix}$$

Applying the change of basis $A'_j = T^{-1}\bar{A}'_j T$, we get that

$$A'_1 = \begin{pmatrix} 5 & 5 & 4 \\ 6 & 1 & 3 \\ 2 & 1 & 0 \end{pmatrix} A'_2 = \begin{pmatrix} 6 & 3 & 0 \\ 3 & 2 & 1 \\ 5 & 2 & 6 \end{pmatrix} A'_3 = \begin{pmatrix} 0 & 2 & 4 \\ 1 & 4 & 0 \\ 6 & 1 & 3 \end{pmatrix}$$

Finally, we choose arbitrary matrices B'_j and C'_j except the fact that the first entry c'^1_j of $C'_j T^{-1}$ and last entry b'^n_j of TB'_j are not zero to fulfill the surjectivity condition (24).

$$B'_1 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, B'_2 = \begin{pmatrix} 1 \\ 2 \\ 5 \end{pmatrix}, B'_3 = \begin{pmatrix} 3 \\ 6 \\ 1 \end{pmatrix}$$

$$C'_1 = (2\ 1\ 3), C'_2 = (6\ 2\ 1), C'_3 = (3\ 1\ 1)$$

Finally, we derive the equations (12) of $\mathcal{C}$. The matrices read

$$A_1 = \begin{pmatrix} 6 & 5 & 4 \\ 6 & 1 & 3 \\ 0 & 0 & 4 \end{pmatrix}, A_2 = \begin{pmatrix} 0 & 1 & 6 \\ 5 & 5 & 6 \\ 3 & 6 & 1 \end{pmatrix}, A_3 = \begin{pmatrix} 5 & 6 & 1 \\ 4 & 5 & 1 \\ 3 & 0 & 2 \end{pmatrix}$$

$$B_1 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, B_2 = \begin{pmatrix} 1 \\ 2 \\ 5 \end{pmatrix}, B_3 = \begin{pmatrix} 3 \\ 6 \\ 1 \end{pmatrix}$$

$$C_1 = (5\ 6\ 4), C_2 = (1\ 5\ 6), C_3 = (4\ 6\ 6)$$

$$D_1 = D_2 = D_3 = 1$$

After the setting is completed, a sequence $\{u\}$ is applied to $\mathcal{C}$. As expected, the self-synchronization is achieved after a finite transient time, so does the recovery of the sequence of inputs (see Figure 3). The transient time before self-synchronization is of length $K = 3$ since the class of nilpotency t of the set (A'_1, A'_2, A'_3) equals 3.

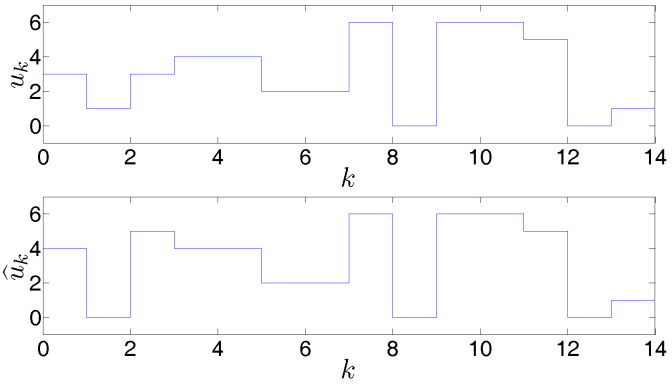

Fig. 3. Time evolution of $\{u\}$ and $\{\widehat{u}\}$ of the setup $\mathcal{C}$-$\mathcal{D}$

REFERENCES

S. Banerjee, editor. *Chaos Synchronization and Cryptography for Secure Communications: Applications for Encryption*. IGI Global, 2010.

I.I. Blekhman, A.L. Fradkov, Nijmeijer H., and A.Y Pogromsky. On self-synchronization and controlled synchronization. *Systems and Control letters*, 31(5):299–305, 1997.

C. Carlet. *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, chap. Vectorial Boolean Functions for Cryptography. Cambridge Press, 2010.

J. Daemen. *Cipher and Hash function design, strategies based on linear and differential cryptanalysis.* PhD Thesis, Katholieke Universiteit Leuven, 1995.

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.

M. Fliess, J. Levine, P. Martin, and P. Rouchon. Flatness and defect of non-linear systems: introductory theory and examples. *Int. J. of Control*, 61(6):1327–1361, 1995.

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.

G. Millérioux and P. Guillot. Self-synchronizing stream ciphers and dynamical systems: state of the art and open issues. *International Journal of Bifurcation and Chaos*, 20(9), September 2010.

G. Millérioux, J. M. Amigó, and J. Daafouz. A connection between chaotic and conventional cryptography. *IEEE Trans. on Circuits and Systems I: Regular Papers*, 55 (6), July 2008.

J. Parriaux, P. Guillot, and G. Millérioux. Synchronization of boolean dynamical systems: a spectral characterization. In Claude Carlet and Alexander Pott, editors, *Sequences and Their Applications (SETA 2010)*, volume 6338 of *Lecture Notes in Computer Science*, Paris, France, September 2010. Springer Berlin / Heidelberg.

H. Radjavi and P. Rosenthal. *Simultaneous Triangularization.* Springer, 2000.

C. B. Schrader and M. K. Sain. Research on system zeros: a survey. *Int. Jour. of Control*, 50(4):1407–1433, 1989.

H. Sira-Ramirez and S. K. Agrawal. *Differentially Flat Systems.* Marcel Dekker, New York, 2004.