Invertibility, flatness and identifiability of switched linear dynamical systems: an application to secure communications

Phuoc Vo Tan, Gilles Millérioux, Jamal Daafouz

Invertibility, flatness and identifiability of switched linear dynamical systems: an application to secure communications

Phuoc Vo Tan, Gilles Millérioux and Jamal Daafouz

***Abstract*— This paper deals with invertibility, flatness and identifiability of switched linear dynamical systems. Based on these concepts, a framework which enables to test whether, from a structural point of view, a switched linear dynamical system can act as a cryptosystem for secure communications is proposed.**

Hybrid systems have inspired a great deal of research from both control theory and theoretical computer science. They provide a strong theoretical foundation which combines discrete-event and continuous-time systems in a manner that can capture software logic and physical dynamics in a unified modeling framework. The most well-known area of applicability of hybrid systems are naturally modeling, analysis and control design of embedded systems. Switched systems are an important class of hybrid systems widely studied in the literature and stability, identifiability, controller or observer design are challenging problems related to. They are usually addressed for engineering applications.

The contribution of this paper is to provide results for an application related to secure communications. Let us briefly describe this context. Chaotic behavior is one of the most complex dynamics a nonlinear system can exhibit. Because the signals resulting from chaotic systems are broadband, noiselike, difficult to predict, the idea of using chaotic systems for information masking has received much attention since the pioneering work of [1]. Several ciphering methods for masking the information into a chaotic signal produced by a dynamical system have been proposed in the literature. An overview can be found according to the chronology in [2][3][4][5].
In this paper, we propose a framework, based on the concepts of control theory, which enables to test whether, from a structural point of view, a switched linear dynamical system can act as a cryptosystem. Such a class is interesting because it combines two advantages: capability of exhibiting complex dynamics and ease of implementation.

The paper is organized as follows. Section I aims at deriving algebraic conditions under which a switched linear discrete-time system is respectively invertible and flat. It is shown how these concepts are useful in the perspective of designing ciphers for secure communications, more precisely self-synchronizing stream ciphers. In Section II the security aspect is addressed and a connection between identification and algebraic attacks is brought out. An illustrative example is finally given.

I. Invertibility, flatness and identifiability

Consider the switched linear dynamical system:

$$\left\{\begin{array}{lcl} x_{k+1} & = & A_{\sigma(k)}x_k + B_{\sigma(k)}u_k \\ y_k & = & C_{\sigma(k)}x_k + D_{\sigma(k)}u_k \end{array}\right. \tag{1}$$

where $x_k \in \mathbb{R}^n$, $u_k \in \mathbb{R}$ and $y_k \in \mathbb{R}$. All the matrices, namely $A_{\sigma(k)} \in \mathbb{R}^{n\times n}$, $B_{\sigma(k)} \in \mathbb{R}^{n\times 1}$, $C_{\sigma(k)} \in \mathbb{R}^{1\times n}$ and $D_{\sigma(k)} \in \mathbb{R}$ 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 $(D_j)_{1\leq j\leq J}$. At a given time k, the index j corresponds to the mode of the system and results from a switching function $\sigma : k \in \mathbb{N} \mapsto j = \sigma(k) \in \{1,\ldots,J\}$. $\{\sigma\}_{k_1}^{k_2}$ refers to the mode sequence $\{\sigma(k_1),\ldots,\sigma(k_2)\}$.
Let $\mathscr{U}$ be the space of input sequences over $[0,\infty)$ and $\mathscr{Y}$ the corresponding output space. At time k, for each initial state $x_k \in \mathbb{R}^n$, when the system (1) is driven by the input sequence $\{u\}_k^{k+T} = \{u_k,\ldots,u_{k+T}\} \in \mathscr{U}$, for a mode sequence $\{\sigma\}_k^{k+T}$, $\{x(x_k,\sigma,u)\}_k^{k+T}$ refers to the solution of (1) starting from x_k in the interval of time $[k,k+T]$ and $\{y(x_k,\sigma,u)\}_k^{k+T} \in \mathscr{Y}$ refers to the corresponding output sequence in the same interval of time $[k,k+T]$.

Two structural properties of (1) are now addressed : invertibility and flatness.

A. Invertibility

Before addressing the invertibility property, the relative degree of a switched linear system must be defined. We first recall a general definition.

Definition 1: The *relative degree* of a dynamical system with respect to its input u_k is the required number r of iterations of its output y_k so as y_{k+r} depends explicitly on u_k.

Remark 1: Hereafter, we only consider the case when the relative degree r is constant.

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

$$y_{k+i} = C_{\sigma(k+i)}A_{\sigma(k)}^{\sigma(k+i-1)}x_k + \sum_{j=0}^{j=i} \mathscr{T}_{\sigma(k)}^{i,j}u_{k+j} \tag{2}$$

The authors are with Nancy University, Centre de Recherche en Automatique de Nancy, France, Phuoc.Vo-Tan@esstin.uhp-nancy.fr, gilles.millerioux@esstin.uhp-nancy.fr, jamal.daafouz@ensem.inpl-nancy.fr

with

$$\mathscr{T}^{i,j}_{\sigma(k)} = C_{\sigma(k+i)} A^{\sigma(k+i-1)}_{\sigma(k+j+1)} B_{\sigma(k+j)} \text{ if } j \le i-1, \ \ \mathscr{T}^{i,i}_{\sigma(k)} = D_{\sigma(k+i)} \tag{3}$$

and with the transition matrix defined as:

$$\begin{array}{rcl} A^{\sigma(k_1)}_{\sigma(k_0)} & = & A_{\sigma(k_1)} A_{\sigma(k_1-1)} \dots A_{\sigma(k_0)} \ \text{ if } \ k_1 \ge k_0 \\ & = & \mathbf{1}_n \ \text{ if } \ k_1 < k_0 \end{array}$$

$\mathbf{1}_n$ being the identity matrix of dimension n.
As a result, the relative degree r of (1) is

- $r = 0$ if $\mathscr{T}^{0,0}_{\sigma(k)} \neq 0$ for all k
- the least integer $r < \infty$ such that for all k

$$\begin{array}{l} \mathscr{T}^{i,j}_{\sigma(k)} = 0 \text{ for } \ i = 0, \dots, r-1 \ \text{ and } \ j = 0, \dots, i \\ \mathscr{T}^{r,0}_{\sigma(k)} \neq 0 \end{array} \tag{4}$$

When (1) has relative degree r, its output reads at time $k+r$:

$$y_{k+r} = C_{\sigma(k+r)} A^{\sigma(k+r-1)}_{\sigma(k)} x_k + \mathscr{T}^{r,0}_{\sigma(k)} u_k \tag{5}$$

Definition 2: The system (1) is *left invertible* if there exists a nonnegative integer $R < \infty$ such that, for two any inputs sequences $\{u\}^{k+R}_k, \{u'\}^{k+R}_k \in \mathscr{U}$, the following implication applies:

$$\forall \sigma, \forall x_k \ \{y(x_k, \sigma, u)\}^{k+R}_k = \{y(x_k, \sigma, u')\}^{k+R}_k \quad \Rightarrow \quad u_k = u'_k \tag{6}$$

In other words, (1) is *left invertible* if the input u_k can be uniquely determined from an output sequence of finite length for any known initial condition and switching rule. It turns out that if (1) has a finite relative degree r, it is also left invertible with $R = r$. Indeed, if (1) has a finite relative degree r, (5) holds and the input u_k can be deduced in a unique way. It reads:

$$u_k = (\mathscr{T}^{r,0}_{\sigma(k)})^{-1} (y_{k+r} - C_{\sigma(k+r)} A^{\sigma(k+r-1)}_{\sigma(k)} x_k) \tag{7}$$

The existence of the inverse of $\mathscr{T}^{r,0}_{\sigma(k)}$ is guaranteed since it is, by definition, always different from zero.

B. Inversion

We are now concerned with a recursive inversion of (1) achieving the recovering of u_k from y_k without any knowledge of x_k. Let us define the inverse transition matrix as

$$\begin{array}{rcl} P^{\sigma(k_1)}_{\sigma(k_0)} & = & P^r_{\sigma(k_1)} P^r_{\sigma(k_1-1)} \cdots P^r_{\sigma(k_0)} \ \text{ if } \ k_1 \ge k_0 \\ & = & \mathbf{1}_n \ \text{ if } \ k_1 < k_0 \end{array}$$

with

$$P^r_{\sigma(k)} = A_{\sigma(k)} - B_{\sigma(k)} (\mathscr{T}^{r,0}_{\sigma(k)})^{-1} C_{\sigma(k+r)} A^{\sigma(k+r-1)}_{\sigma(k)} \tag{8}$$

Proposition 1: The following dynamical system is a stable inverter whenever the system $v_{k+1} = P^r_{\sigma(k)} v_k$ is uniformly asymptotically stable

$$\left\{ \begin{array}{rcl} \hat{x}_{k+r+1} & = & P^r_{\sigma(k)} \hat{x}_{k+r} + B_{\sigma(k)} (\mathscr{T}^{r,0}_{\sigma(k)})^{-1} y_{k+r} \\ \hat{u}_{k+r} & = & -(\mathscr{T}^{r,0}_{\sigma(k)})^{-1} C_{\sigma(k+r)} A^{\sigma(k+r-1)}_{\sigma(k)} \hat{x}_{k+r} \\ & & +(\mathscr{T}^{r,0}_{\sigma(k)})^{-1} y_{k+r} \end{array} \right. \tag{9}$$

Proof: On one hand, substituting (5) into (9) yields:

$$\begin{array}{rcl} \hat{x}_{k+r+1} & = & P^r_{\sigma(k)} \hat{x}_{k+r} + B_{\sigma(k)} (\mathscr{T}^{r,0}_{\sigma(k)})^{-1} C_{\sigma(k+r)} A^{\sigma(k+r-1)}_{\sigma(k)} x_k \\ & & + B_{\sigma(k)} (\mathscr{T}^{r,0}_{\sigma(k)})^{-1} \mathscr{T}^{r,0}_{\sigma(k)} u_k \end{array} \tag{10}$$

Taking into account (8) and noticing that $(\mathscr{T}^{r,0}_{\sigma(k)})^{-1} \mathscr{T}^{r,0}_{\sigma(k)} = 1$, $\varepsilon_k = x_k - \hat{x}_{k+r}$ fulfills the recursion:

$$\begin{array}{rcl} \varepsilon_{k+1} & = & (A_{\sigma(k)} - B_{\sigma(k)} (\mathscr{T}^{r,0}_{\sigma(k)})^{-1} C_{\sigma(k+r)} A^{\sigma(k+r-1)}_{\sigma(k)}) \varepsilon_k \\ & & = P^r_{\sigma(k)} \varepsilon_k \end{array} \tag{11}$$

On the other hand, from the expression (7) of u_k and the expression of $\hat{u}_{k+r}$ in (9), we get that:

$$u_k - \hat{u}_{k+r} = -(\mathscr{T}^{r,0}_{\sigma(k)})^{-1} C_{\sigma(k+r)} A^{\sigma(k+r-1)}_{\sigma(k)} (x_k - \hat{x}_{k+r}) \tag{12}$$

From (12) we can infer that $\hat{u}_{k+r}$ converges toward u_k as long as $\hat{x}_{k+r}$ converges toward x_k, that is provided that the system $v_{k+1} = P^r_{\sigma(k)} v_k$ with $v_k = \varepsilon_k$ is uniformly asymptotically stable.

■

C. Flatness

We first recall a general definition of *flat output* (for details about flatness, the reader can refer to [6] or the book [7]).

Definition 3: A *flat output* of a dynamical system is an output variable y_k such that all system variables can be expressed as a function of y_k and a finite number of its forward/backward iterates. In particular, there exists two functions $\mathscr{F}$, $\mathscr{G}$ and integers $t_1 < t_2$, $t'_1 < t'_2$ such that

$$\begin{array}{rcl} x_k & = & \mathscr{F}(y_{k+t_1}, \cdots, y_{k+t_2}) \\ u_k & = & \mathscr{G}(y_{k+t'_1}, \cdots, y_{k+t'_2}) \end{array} \tag{13}$$

We derive an algebraic interpretation of flat outputs for (1).

Proposition 2: The output y_k of (1), assumed to be left invertible, is a flat output if there exists a positive integer $0 < K < \infty$ such that for all $k \ge 0$

$$P^{\sigma(k+K-1)}_{\sigma(k)} = \mathbf{0} \tag{14}$$

where $\mathbf{0}$ stands for the null matrix.
Proof: The proof is based on the inverse system. Iterating (9) $l-1$ times yields:

$$\begin{array}{rcl} \hat{x}_{k+r+l} & = & P^{\sigma(k+l-1)}_{\sigma(k)} \hat{x}_{k+r} \\ & & + \sum_{i=0}^{l-1} P^{\sigma(k+l-1)}_{\sigma(k+i+1)} B_{\sigma(k+i)} \mathscr{T}^{r,0}_{\sigma(k+i)} y_{k+i+r} \end{array} \tag{15}$$

If (14) is fulfilled, (15) turns into

$$\hat{x}_{k+r+K} \ = \ \sum_{i=0}^{K-1} P^{\sigma(k+K-1)}_{\sigma(k+i+1)} B_{\sigma(k+i)} \mathscr{T}^{r,0}_{\sigma(k+i)} y_{k+i+r} \tag{16}$$

revealing that $\hat{x}_{k+r+K}$ is independent of $\hat{x}_{k+r}$. In particular, (16) holds for $\hat{x}_{k_0+r} = x_{k_0}$ for all $k_0 \ge 0$, that is for $\varepsilon_{k_0} = 0$ with $k_0 \ge 0$. By virtue of (11), we infer that $\varepsilon_k = 0$ for all $k \ge k_0$ and thus $\hat{x}_{k+r+K} = x_{k+K}$ for all $k \ge 0$. Therefore, after performing the change of variable $k \to\ k-K$, we obtain an explicit form for $\mathscr{F}$ involved in (13).

$$x_k \quad = \quad \sum_{i=0}^{K-1} P_{\sigma(k+i+1-K)}^{\sigma(k-1)} B_{\sigma(k+i-K)} \mathscr{T}_{\sigma(k+i-K)}^{r,0} y_{k+i+r-K} \tag{17}$$

On the other hand, substituting (17) into (7) yields an explicit form for $\mathscr{G}$ involved in (13) and then, we infer that y_k is a flat output according to the Definition 3.

■

D. Connection with usual stream ciphers in secure communication

Secure communications requires cryptographic algorithms called ciphers (see the book of Menezes [8] for details). Among a variety of ciphers, symmetric-key ciphers are very efficient for secure transmission requiring high throughput. We focus here on self-synchronous stream ciphers which is an interesting class of symmetric ciphers owing to their inherent ability to self-synchronizing without requiring any synchronization flags or interactive protocols for recovering lost synchronization induced for instance by bit slips. At the transmitter side, the self-synchronous stream cipher admits the following recursion, written with the usual notation encountered in the literature:

$$\left\{ \begin{array}{l} K_k = \sigma_\theta^{ss}(c_{k-l}, \ldots, c_{k-l'}) \\ c_{k+b_s} = e(K_k, m_k) \end{array} \right. \tag{18}$$

m_k is the information to be encrypted and is called the plaintext. c_k is the encrypted information and is called the ciphertext which is conveyed through a public channel to the receiver. The ciphertext is delivered by the encryption function e depending on the so-called time-varying key K_k also named keystream. σ_θ^{ss} is a function, parameterized by a parameter vector θ that is the secret key, that generates the keystream. σ_θ^{ss} depends on c_{k-i} $(i = l, \ldots, l')$ that is a fixed number of past values of c_k. b_s is a positive integer. When strictly greater than zero, b_s corresponds to a delay between the plaintext m_k and the corresponding ciphertext c_{k+b_s}. This delay is due to a sequential computation of the ciphertext through an architecture which involves a pipeline with b_s stages (see for example the algorithm called Mosquito [9]). Actually, (18) is a conceptual model, called canonical representation, that may correspond to numerous different architectures.

From the results of Subsect. I-A and Subsect. I-C concerning invertibility and flatness, we are in position of providing some conditions under which (1) may act as a self-synchronizing stream cipher.

Proposition 3: If (1) has a finite relative degree r and y_k is a flat output, then (1) is a self-synchronizing stream cipher.

Proof: By virtue of (5) and (17), the system (1) can be rewritten in the following equivalent form:

$$\left\{ \begin{array}{lcl} x_k & = & \sum_{i=0}^{K-1} P_{\sigma(k+i+1-K)}^{\sigma(k-1)} B_{\sigma(k+i-K)} \mathscr{T}_{\sigma(k+i-K)}^{r,0} y_{k+i+r-K} \\ y_{k+r} & = & C_{\sigma(k+r)} A_{\sigma(k)}^{\sigma(k+r-1)} x_k + \mathscr{T}_{\sigma(k)}^{r,0} u_k \end{array} \right. \tag{19}$$

and the result follows from the identification of (19) with (18), the correspondences being:

- $u_k \leftrightarrow m_k$ (plaintext)
- $y_k \leftrightarrow c_k$ (ciphertext)
- $x_k \leftrightarrow K_k$ (keystream)
- $\mathscr{F} \leftrightarrow \sigma_\theta^{ss}$ (keystream generator)
- $(x_k, u_k) \mapsto C_{\sigma(k+r)} A_{\sigma(k)}^{\sigma(k+r-1)} x_k + \mathscr{T}_{\sigma(k)}^{r,0} u_k \leftrightarrow e$ (encryption function)
- $r \leftrightarrow b_s$ (number of stages of the pipeline)

■

II. Identification, algebraic attacks and security

An essential issue for the validation of cryptosystems is the cryptanalysis, that is the study of attacks against cryptographic schemes in order to reveal their possible weakness. A fundamental assumption in cryptanalysis, first stated by A. Kerkhoff in [10], is that the eavesdropper knows all the details of the cryptosystem, including the algorithm and its implementation, except the secret key, on which the security of the cryptosystem must be entirely based. As a result, the security is directly related to the complexity of the parameters recovering task and so, on the complexity of the underlying identification procedure. The identification is nothing but what is called in the cryptographic context an algebraic attack. The consideration of the possible attacks and their complexity will dictate the way how the secret key of (1) must be defined as detailed below.

A. Connection between identification and algebraic attacks

One of the most powerful attack is the chosen plaintext attack. For such an attack, the eavesdropper is assumed to control the input of the cipher, namely the plaintext, and to analyze the corresponding ciphertext. In our context, since the cipher is the dynamical system (1), it means that the eavesdropper is supposed to control both the input u_k and the output y_k. As a result, the pair (u_k, y_k) is supposed to be known by the eavesdropper and the cryptanalytic reasoning must be based on the input/output model of (1).

When the switched system (1) is flat, its input/output model can be obtained in a systematic way. Indeed, if (1) is flat with flat output y_k, the state vector x_k obeys (17). Substituting the expression (17) of x_k into (5) yields

$$y_{k+r} = C_{\sigma(k+r)} A_{\sigma(k)}^{\sigma(k+r-1)} \cdot \left(\sum_{i=0}^{K-1} P_{\sigma(k+i+1-K)}^{\sigma(k-1)} B_{\sigma(k+i-K)} \mathscr{T}_{\sigma(k+i-K)}^{r,0} y_{k+i+r-K}\right) + \mathscr{T}_{\sigma(k)}^{r,0} u_k \tag{20}$$

Let $\{\sigma_1\}_{k+r-K}^{k+r-1}, \ldots, \{\sigma_N\}_{k+r-K}^{k+r-1}$ the N possible mode sequences $\{\sigma(k+r-K), \ldots, \sigma(k+r-1)\}$ over the interval of time $[k+r-K, k+r-1]$. The number N of all possible mode sequences is finite since the number J of modes of

(1) is. These mode sequences will be respectively denoted for short $\sigma_1,\dots,\sigma_N$ in the sequel. Thus, for $t=1,\dots,N$, the input/output relation (20) can be rewritten as

$$y_{k+r}=\sum_{j=0}^{K-1} a_j(\sigma_t)y_{k+j+r-K}+c(\sigma_t)u_k \tag{21}$$

where $c(\sigma_t)$ and the $a_j(\sigma_t)$'s $(j=0,\dots,K-1)$ are coefficients depending in different ways according to the sequence σ_t on the entries of the matrices $(A_j)_{1\leq j\leq J}$, $(B_j)_{1\leq j\leq J}$, $(C_j)_{1\leq j\leq J}$ and $(D_j)_{1\leq j\leq J}$ of (1)

Let us first assume that σ_t is accessible. Since for each σ_t, the parameters $c(\sigma_t)$ and the $a_j(\sigma_t)$'s appear in a linear fashion in the input/output relation (21), they are obviously identifiable. Indeed, for a given mode sequence σ_t, under the usual Persistently Exciting (PE) conditions, the identification can always be performed by iterating the relation (21) until a set of linear independent equations is obtained. The solution is unique for each σ_t and gives $c(\sigma_t)$ and the $a_j(\sigma_t)$'s.

Conversely, let us assume that σ_t is not accessible. The previous procedure does no longer hold. An alternative identification procedure (and so algebraic attack) for recovering $c(\sigma_t)$ and the $a_j(\sigma_t)$'s attack can follow the method proposed in [11] for switched ARX systems. This method is summed up and adapted to our context.
Each input/output relation (21) can be rewritten for $t=1,\dots,N$

$$z_k^T b_t=0 \tag{22}$$

- $z_k=[y_{k+r},y_{k+r-1},\cdots,y_{k+r-K},u_k]^T\in\mathbb{R}^{K+2}$
- $b_t=[1,-a_0(\sigma_t),\dots,-a_{K-1}(\sigma_t),-c(\sigma_t)]^T\in\mathbb{R}^{K+2}$

z_k is the *regressor vector* while b_t is the *parameter vector* corresponding to the mode sequence σ_t.
We can thereby define N hyperplanes S_t, $t=1\dots,N$

$$S_t=\{z_k : z_k^T b_t=0\}$$

The key idea rests on the fact that the so-called *Hybrid Decoupling Constraint* equation is fulfilled regardless the switching sequences:

$$p_N(z_k)=\prod_{t=1}^{N}(z_k^T b_t)=\nu_N(z_k)^T h_N=0 \tag{23}$$

$h_N\in\mathbb{R}^{M_N}$ is the coefficient of the *Hybrid Decoupling Polynomial* and $\nu_N : z_k\in\mathbb{R}^{K+2}\mapsto\xi_k\in\mathbb{R}^{M_n}$ is a *Veronese map* of degree N, the components of ξ_k corresponding to all the M_N monomials (product of the components of z_k) sorted in the degree-lexicographic order. The quantity M_N is given by

$$M_N=\left(\begin{array}{c} N+K-1 \\ N \end{array}\right)=\frac{(N+K-1)!}{N!(K-1)!} \tag{24}$$

For the identification of the b_t's in (22), it is needed to compute the coefficients h_N of (23). To this end, let $\mathscr{L}_N$ denote an embedded data matrix involving N mapped regressor vectors z_k through ν_N

$$\mathscr{L}_N=\left[\begin{array}{c} \nu_N(z_{k_1}) \\ \nu_N(z_{k_2}) \\ \dots \\ \nu_N(z_{k_N}) \end{array}\right]^T\in\mathbb{R}^{N\times M_N}$$

The following relation applies:

$$\mathscr{L}_N h_N=\mathbf{0} \tag{25}$$

If the mapped regressor vectors $\nu_N(z_{k_i})$'s are *sufficiently exciting*, the existence of an integer N' such that the $\nu_{N'}(z_{k_i})$'s $(i=1,\dots,N')$ can span a M_N-1 dimensional vector space, i.e

$$rank(\mathscr{L}_{N'})=(M_N-1) \tag{26}$$

is guaranteed. The lower bound of N' is M_N-1. If (26) is fulfilled, the coefficient h_N can be retrieved by

$$h_N=Ker(\mathscr{L}_{N'}) \tag{27}$$

Finally, to recover the parameter vectors b_t from the knowledge of h_N, let's consider the derivative $Dp_N(z_k)$ of $p_N(z_k)$:

$$Dp_N(z_k)=\frac{\partial p_N(z_k)}{\partial z_k}=\frac{\partial}{\partial z_k}\prod_{t=1}^{N}(z_k^T b_t)=\sum_{t=1}^{N} b_t\prod_{l\neq t}(z_k^T b_l) \tag{28}$$

If w_t is a point lying on the t^{th} hyperplane S_t, we can obtain, for $t=1,\dots,N$, the b_t's by performing:

$$b_t=\frac{Dp_N(w_t)}{eDp_N(w_t)} \tag{29}$$

e stands for the vector $[1\ 0\cdots 0]\in\mathbb{R}^{K+2}$.

Remark 2: An algebraic solution to determine the N distinct points w_t that lie on the N hyperplanes S_t can be found in [11].

B. Complexity and security

We recall that the parameters $c(\sigma_t)$ and $a_j(\sigma_t)$'s of the input/output model of (1) depend on the entries of the matrices $(A_j)_{1\leq j\leq J}$, $(B_j)_{1\leq j\leq J}$, $(C_j)_{1\leq j\leq J}$ and $(D_j)_{1\leq j\leq J}$ and on the switching rule σ. The objective of this section is to determine the relevant entries of the matrices which can be involved in the secret key denoted hereafter θ.

To this end, it worth emphasizing that a cryptosystem must face at least the most basic attack, i.e. the brute force attack. This attack consists in trying exhaustively every possible parameter value in the parameter space of the secret key (which is in practice a finite space). The quicker the brute force attack, the weaker the cryptosystem. Consequently, the worst situation for the eavesdropper and the best for the security arises when, for known plaintexts (because accessible to eavesdropper in the chosen plaintext attack) and corresponding ciphertext sequences, only one solution in the parameters of the cipher exists.

And yet, we recall that a component $\theta^{(i)}$ of a parameter vector θ of a discrete-time dynamical system is *identifiable* if $\theta^{(i)}$ can be rewritten as a unique function φ of the input, the output and their iterates

$$\theta^{(i)} = \varphi(y_k, \ldots, y_{k+M}, u_k, \ldots, u_{k+M'}) \qquad (30)$$

with $M < \infty$ and $M^{'} < \infty$ some positive integers.
As a result, we conclude that the most relevant parameters of a system to act as the secret key are the ones which are identifiable (a result which could seem paradoxical at first glance without the previous reasoning).

From the identification procedures described above, it turns out that $c(\sigma_t)$ and the $a_j(\sigma_t)$'s ($j = 0, \ldots, K-1,\ t = 1, \ldots, N$) can always be expressed in a unique way as a function of the input, the output and their iterates. Thus we have the following result:

Proposition 4: The secret key θ must be the set of entries of $(A_j)_{1\leq j\leq J}$, $(B_j)_{1\leq j\leq J}$, $(C_j)_{1\leq j\leq J}$ and $(D_j)_{1\leq j\leq J}$ of (1) which can be deduced from $c(\sigma_t)$ and the $a_j(\sigma_t)$'s in a unique way.

Besides, it has been seen that if σ_t is accessible, recovering the parameters $c(\sigma_t)$ and $a_j(\sigma_t)$'s of the input/output model is quite simple by solving a set of linear equations. Thus to force the eavesdropper resorting to the second approach and so to complexify the identification, one must imagine a configuration for which σ_t is not directly accessible. One solution is to render the switching rule σ dependent on θ as well.

We are now in position of assessing the security in terms of the complexity of the required algebraic computations to identify θ. The most important task in the algebraic procedure related to the case σ_t not accessible and described above is the computation of the coefficients h_N through (27). In practice, the kernel (null space) is obtained through a Singular Values Decomposition (SVD) of which complexity is $O(min(N'M_N^2, N'^2M_N))$. The lower bound of N' being $M_N - 1$, when M_N is large enough, the complexity can be approximated by $O(M_N)^3$. The increasing rate of M_N is depicted on Figure 1. Similarly to all existing ciphers, the complexity obviously increases with the number of parameters in the key space. What is important is the way how the complexity increases with respect to the number of parameters. A bad algorithm is a one for which the complexity increases linearly with respect to the number of parameters. The above study shows that it is not the case for piecewise linear systems and highlights the potential relevance of resorting to such class of systems for cryptographic purposes. As an example, take $N = 32$ and $K = 6$, then $M_N = 435897$. The minimum number of iterations for checking the rank condition (26) is 435897^3. Let us assume that each iteration takes $10^{-9}s$, we will spend nearly $2,62$ years to retrieve the parameters!

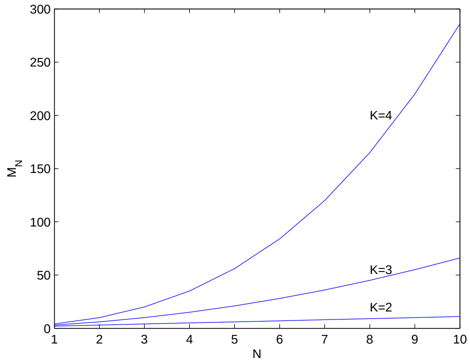

Fig. 1. M_N versus N for different values of K.

C. *Illustrative example*

We consider a switched linear system in the form (1) with

$$A_{\sigma(k)} = \begin{pmatrix} q^1_{\sigma(k)} & 1 \\ 0.5 & 0 \end{pmatrix}, \quad B_{\sigma(k)} = \begin{pmatrix} 0 \\ q^2_{\sigma(k)} \end{pmatrix}$$

and with $C_{\sigma(k)} = (1\ 0)$ and $D_{\sigma(k)} = 0$ for any k.

The number of modes of the switching rule σ is $J = 4$. The time-varying entries fulfill $q^1_1 = q^1_2 = 1.7$, $q^1_3 = q^1_4 = -1.7$, $q^2_1 = q^2_3 = -0.01$, $q^2_2 = q^2_4 = 0.01$.

Structural consideration

i) The relative degree is $r = 2$ according to (4) since $\mathscr{T}^{i,j}_{\sigma(k)} = 0$ for $i = 0,1$ and $j = 0, \ldots, i$. Besides $\mathscr{T}^{2,0}_{\sigma(k)} = C_{\sigma(k+2)}A_{\sigma(k+1)}B_{\sigma(k)} \neq 0$ for all k.
ii) The computation of (14) gives $\mathbf{0}$ with $K = 2$ and reveals that y_k is a flat output.
From *i)* and *ii)*, we can infer that the system is a self-synchronizing stream cipher according to the Proposition 3.

Determination of the secret key

iii) For the secret key, we choose $\theta = (\theta^{(1)}\ \ \theta^{(2)}\ \ \theta^{(3)}\ \ \theta^{(4)}\ \ \theta^{(5)}) = (q^1_1\ \ q^1_3\ \ q^3\ \ q^2_1\ \ q^2_2) = (1.7\ \ -\ 1.7\ \ 0.5\ \ -\ 0.01\ \ 0.01)$ of dimension $L = 5$. Let us check whether it is an admissible choice in terms of identifiability.

The computation of (20) allows us to obtain an input/output relation in the form of (21)

$$\begin{aligned} y_{k+2} &= 0.5y_k + q^1_{\sigma(k+1)}y_{k+1} + q^2_{\sigma(k)}u_k \\ &= a_0(\sigma_t)y_k + a_1(\sigma_t)y_{k+1} + c(\sigma_t)u_k \end{aligned} \qquad (31)$$

In the time interval $[k, k+1]$, to the $N = 4$ possible modes sequences $\sigma_1 = \{1,1\}$, $\sigma_2 = \{1,2\}$, $\sigma_3 = \{2,1\}$, $\sigma_4 = \{2,2\}$, correspond four respective input/output equations

$$\begin{aligned} t = 1, \quad y_{k+2} &= \theta^{(3)}y_k + \theta^{(1)}y_{k+1} + \theta^{(4)}u_k \\ t = 2, \quad y_{k+2} &= \theta^{(3)}y_k + \theta^{(2)}y_{k+1} + \theta^{(4)}u_k \\ t = 3, \quad y_{k+2} &= \theta^{(3)}y_k + \theta^{(1)}y_{k+1} + \theta^{(5)}u_k \\ t = 4, \quad y_{k+2} &= \theta^{(3)}y_k + \theta^{(2)}y_{k+1} + \theta^{(5)}u_k \end{aligned}$$

with the following relations

$$\begin{array}{l}\theta^{(1)} = a_1(\sigma_1) \text{ or } \theta^{(1)} = a_1(\sigma_3) \\ \theta^{(2)} = a_1(\sigma_2) \text{ or } \theta^{(2)} = a_1(\sigma_4) \\ \theta^{(3)} = a_0(\sigma_t) \text{ for any } t = 1, \dots, 4 \\ \theta^{(4)} = c(\sigma_1) \text{ or } \theta^{(4)} = c(\sigma_2) \\ \theta^{(5)} = c(\sigma_3) \text{ or } \theta^{(5)} = c(\sigma_4)\end{array} \quad (32)$$

From (32), we infer that θ can be recovered in a unique way from the knowledge of $(a_0(\sigma_t), a_1(\sigma_t), c(\sigma_t))$ $(t = 1, \dots, 4)$ and then Proposition 4 is fulfilled. Consequently θ can act as the secret key.

Attack and related complexity

iv) Let us perform the algebraic attack described in Subsect. II-B and assess its complexity. To this end, we inject known plaintexts u_k into (1) and collect the corresponding ciphertexts y_k. We then iterate (1) until a sufficient number of regressor vectors z_{k_i} are obtained for the matrix $\mathscr{L}_{N'}$ to fulfill the rank condition (26). After computing h_N from (27), we derive $b_1, \dots, b_4$ by (29)

$$\begin{array}{rlrrr} b_1 = & [1 & \text{-0.5} & -1.7 & 0.01]^T \\ b_2 = & [1 & \text{-0.5} & 1.7 & 0.01]^T \\ b_3 = & [1 & \text{-0.5} & -1.7 & -0.01]^T \\ b_4 = & [1 & \text{-0.5} & 1.7 & -0.01]^T \end{array}$$

and then recover the $c(\sigma_t)$'s and the $a_j(\sigma_t)$'s $(j = 0, \dots, K-1,\ t = 1, \dots, N)$ and finally the $\theta^{(i)}$'s by (32). According to the discussion of Subsect. II-B, it is worth emphasizing that since $M_4 = 35$, the minimal complexity of the attack is $35^3 = 42875$, a complexity which would have required a dimension 35 if we would have resorted to a linear system.

III. Conclusion

In this paper, it is presented a framework which enables to test whether a switched linear system may act as a self-synchronizing cryptosystem from a structural point of view. Invertibility and flatness are the two properties which allow the dynamical system to be structurally equivalent to a self-synchronizing stream cipher. Identifiability is the necessary required property such that the parameters may be involved in the secret key. Identification consists of an algebraic attack in the context of secure communication. For switched linear systems, the complexity to identify the parameters increases significantly with the number of modes and let us expect that switched linear systems could be good candidates for ciphering. Further consideration are needed for validation in particular the vulnerability against statistical attacks.

Acknowledgement This work is partially funded by a grant from the Agence Nationale pour la Recherche in France (Ref. ANR-05-JCJC-0112-01)

References

[1] T. L. Carroll. and L. M. Pecora, "Synchronizing chaotic circuits," *IEEE Trans. Circuits and Systems*, vol. 38, no. 4, pp. 453–456, April 1991.

[2] M. J. Ogorzalek, "Taming chaos - part I: synchronization," *IEEE Trans. Circuits. Syst. I: Fundamental Theo. Appl*, vol. 40, no. 10, pp. 693–699, 1993.

[3] M. Hasler, "Synchronization of chaotic systems and transmission of information," *International Journal of Bifurcation and Chaos*, vol. 8, no. 4, April 1998.

[4] T. Yang, "A survey of chaotic secure communication systems," *Int. J. of Computational Cognition*, 2004, (available at http://www.YangSky.com/yangijcc.htm).

[5] G. Millérioux, J. M. Amigó, and J. Daafouz, "A connection between chaotic and conventional cryptography," *IEEE Trans. on Circuits and Systems I: Regular Papers*, vol. 55, no. 6, July 2008.

[6] M. Fliess, J. Levine, P. Martin, and P. Rouchon, "Flatness and defect of non-linear systems: introductory theory and examples," *Int. Jour. of Control*, vol. 61, no. 6, pp. 1327–1361, 1995.

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

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

[9] 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.

[10] H. Delfs and H. Knebl, *Introduction to cryptography*. Berlin: Springer-Verlag, 2002.

[11] R. Vidal, Y. Ma, and S. Sastry, "An algebraic geometric approach to the identification of a class of linear hybrid systems," *42nd IEEE Conference on Decision and Control 2003 (CDC'03)*, 2003.